



Cyber Security Innovation Network Funded Project Posters

2023-2025

www.ncc-cnc.ca



Cyber Security Innovation Network Funded Project Posters

This document showcases the projects funded by the Cyber Security Innovation Network (CSIN) program between 2023 - 2025, and separates the projects into a variety of categories. These categories include: theme, province/territory, funding stream, and focus area.

This document can be used to easily and efficiently navigate the project posters.

How to Use This Document

The table of contents of this document links to each category, along with each specific project poster, and will direct you to the desired page by clicking on the category or project title.

There are redundancies within the categories, and each project poster can be found linked under multiple groupings.

Contents

By Theme

Critical infrastructure

- 2023-1496 Building cyber resilient and secure 5G networks through automation and AI
- 2024-1263 Évaluation de la cybersécurité de modèles prédéploiement de systèmes industriels (Poster Title: Cybersecurity Assessment of Pre-deployment Models of Industrial Systems)
- 2024-1282 End-to-end Cyber-Security Solution for the Power Grid
- 2024-1322 ICS Security in the Age of Industry 4.0
- 2024-1360 Adaptive Decision Defense System (ADDS): A Proactive Approach to Detecting and Mitigating Dual Denial of Decision Attacks in Critical Infrastructure
- 2024-1458 Boosting the Cyber-Resilience of Microgrids within Future Energy Critical Infrastructures
- 2024-1470 Ensuring Mission-Critical Security: Coordination of Autonomous Drone Groups with Security-Aware Decision Making

- 2025-1584 Cybersecurity, Resilience, and Trustworthiness of Networked Critical Infrastructure and Autonomous Advanced Air Mobility (AAM) Assets Against Malicious Adversary Cyber-Attacks (Poster Title: Cybersecurity of Autonomous and Advanced/Urban/Electrified Urban Air Mobility (AAM/UAM/EAM))
- 2025-1643 Digital Twin Platform for Critical Infrastructure Cybersecurity Modeling and Assessment (Poster Title: Digital Twin Platform for Cybersecurity Critical Infrastructure)
- 2025-1660 MATSEC: Materials-based Cybersecurity in Electronics (no poster provided)
- 2025-1663 Zero-Knowledge Threat Detection and Risk Assessment in Aerospace and Orbital Infrastructures
- 2025-1690 Protecting Alberta & Nunavut HigherEd with Global Partnerships

Cybersecurity technology

- 2023-1482 Next Generation User Fingerprinting for Fraud Detection and Prediction
- 2023-1487 Trustworthy AI-based Framework for Self-aware Drone-based Swarm Technologies (Poster Title: GPS Spoofing Detection Using Online Federated TinyML for UAV Swarms)
- 2023-1488 Transfer Fuzzing for Devices Without Firmware
- 2023-1492 Cybersécurité de l'identité numérique (Poster Title: Automatic Generation of Decentralized SSI Architectures)
- 2023-1494 PASCAL (Poster Title: PASCALProject: Defending Canada's Infrastructure with Physics-Based Supply Chain Security)
- 2023-1495 Designing a Scalable and Performant Confidential Backup System (no poster provided)
- 2023-1499 The run-time security of Android Automotive infotainment system (no poster provided)
- 2024-1301 Combatting Cyber Influence Operations in Online Social Media (no poster provided)
- 2024-1302 Fully Automated End-to-End Vulnerability Discovery and Repair with LLMs
- 2024-1338 Adaptive Defense Strategies for Advanced Driver-assistance Systems: A Game-theoretic Approach (no poster provided)
- 2024-1356 Toward a Secure User-centric Green Credit Management System (no poster provided)

- 2024-1361 Enhancing Electric Vehicle Charging Infrastructure Cybersecurity Through Autonomous and Sustainable AI
- 2024-1365 Fortifying Cybersecurity: Early Ransomware Detection and Mitigation methods
- 2025-1721 Threat Modelling and Mitigation of human-factors based exploits in advanced driver assistance systems
- 2025-1753 Efficiency and Security of Unknown Group Order Cryptography

Defence, Arctic and sovereignty

- 2024-1326 SCMS: Securing Critical Marine Systems (Poster Title: Marine Cybersecurity)
- 2024-1351 Protecting Democracy from Cyber Threats
- 2024-1372 C1R3 Commercialization (Poster Title: CitizenOne)
- 2024-1428 IntruderInsight: Elevating Cyber Attribution with AI Insights
- 2025-1647 CYBERDEFENSE AI Go-To-Market 2025-2027
- 2025-1689 Securing the Canadian software supply chain (Poster Title: Security Patch-Related regressions in Software Supply Chain)

Privacy

- 2023-1489 Mitigating Security, Privacy, and Ethical Impacts in Driver Assistance Systems (no poster provided)
- 2024-1261 Enabling secure outsourcing of sensitive data (Poster Title: Designing a scalable oblivious Database)
- 2024-1308 Securing the Metaverse with Blockchain and Continuous Authentication Methods (Poster Title: Securing the Metaverse with Multimodal Access Control and Authentication Methods)
- 2024-1345 Secure Genomic Data Processing: Unleashing the Potential of Personalized Medicine (Poster Title: Secure Genomic Data Processing)
- 2024-1346 Ostrich Accounting: Dotting i's and crossing t's with your head in the sand (no poster provided)
- 2024-1386 Preserving Relationship Privacy in Large Networks
- 2024-1418 Novel methods for quantifying and improving privacy in machine learning
- 2024-1433 Enterprise-scale Zero Trust Platform for Privacy-enhancing Smart Metering Services (no poster provided)
- 2024-1439 Privacy Assurance for Canadian Children: A Safe and Secure Framework for Large Language Models (Poster Title: A Human-Centric

Framework for Managing Children's Privacy in Large Language Model Platforms)

- 2025-1548 Secure Healthcare Data Federation through Generative Access Control
- 2025-1770 The Location Dragnet (no poster provided)

Quantum

- 2023-1498 Post-Quantum Hardware Security Module (HSM) Migration Research Project (no poster provided)
- 2024-1305 Authentication for quantum-enabled secure communication (no poster provided)
- 2025-1610 Frontier Quantum-AI Cyber Defense: Pioneering Unprecedented Security Measures for Critical Infrastructure (Poster Title: Quantum-AI Security Framework for Critical Infrastructure and OT/IoT Systems)
- 2025-1778 Post Quantum Resilience of Cyber-Physical Power Systems

Secure AI

- 2023-1519 AI-enabled vulnerability management (no poster provided)
- 2023-1521 ATLAS (no poster provided)
- 2024-1381 Adaptive AI Firewall Specializing in the Protection of AI Models, Critical Infrastructure, Systems, and Agents
- 2024-1409 Transformative Adversaries: Leveraging Generative Pretrained Transformers (GPTs) for the Development of Next-Generation Metamorphic Malware Engines (no poster provided)
- 2024-1454 Revolutionizing Personal Cyber Security with AI-driven Insights (no poster provided)
- 2025-1585 Prescriptive Analysis & Agentic Solutions for Disinformation & Digital Attacks (no poster provided)
- 2025-1601 Self-Healing AI Security via Autonomous Patch Generation & LLM Autovaccination
- 2025-1630 Cyber-Synthetic Risk: A Generative Multi-Agent Approach to Forecasting Advanced Cyberattack Impacts on Enterprise Ecosystems
- 2025-1649 Securing Agentic AI Systems Across the Development and Operations Lifecycle
- 2025-1650 Securing LLM Agents Against Malicious or Vulnerable Tools (Poster Title: Securing AI Agents Against Malicious or Vulnerable Tools)

- 2025-1657 Differential Programming and Fully-Homomorphic Encryption at the Edge
- 2025-1695 Vulnerabilities and Defences of Online Interactive Discussion Forums to Interference by Generative AI (Poster Title: Protecting Democratic Discourse from GenAIChatbots Posing as Humans)
- 2025-1703 AI-Driven IoT Threat Intelligence: Securing Smart Environments Across Zigbee, Z-Wave, Bluetooth, and Wi-Fi Networks (Poster Title: AI-Driven IoT Threat Intelligence)
- 2025-1707 Cyber Resilient Battery Management System with secure Bi-directional Power Flow for Connected Vehicles
- 2025-1759 Reliable and Explainable Malware Detection (Poster Title: Reliable Machine Learning for Android Malware Detection)

Talent and workforce development

- 2023-1485 Mobilizing Cybersecurity Regulation for Canada
- 2023-1486 CyberLab
- 2023-1491 Hybrid Master's Program in Cybersecurity Analytics
- 2023-1493 Cloud Security Training Program (Micro-credential) (no poster provided)
- 2023-1497 Master in Cybersecurity Management (Poster Title: Cybersecurity Management Master)
- 2023-1523 CMD-CT: Comprehensive MultiDisciplinary Cybersecurity Training (no poster provided)
- 2023-1797 De la formation à la cyberstart-up innovante (no poster provided)
- 2024-1242 Accelerating Efforts to Secure Canada in an Era of Quantum
- 2024-1288 Human-Centric Immersive Cybersecurity Training: Socio-Technical and Legal Implications of an Attack
- 2024-1354 MCT: Marine Cybersecurity Training (Poster Title: Marine Cybersecurity)
- 2024-1358 CRAFT: Cybersecure Robotics and Future Talent (no poster provided)
- 2024-1359 IncidentSync: Bridging IT and Law Enforcement
- 2024-1375 Security Awareness Training through Online Social Learning - "From Phishing through Smishing to Vishing" (Poster Title: Phishing, Smishing, Vishing)

- 2024-1423 Formation pour une cybersécurité proactive et interdisciplinaire en entreprise (Poster Title: Parcours Cyber Action: Cybersecurity Training for SMEs)
- 2024-1469 CyberGuardian: Bridging the Cybersecurity Enforcement Training Gap
- 2025-1541 May We Have Your Attention Please? Exploring How Employee Attention Influences Cybersecurity Behaviour (Poster Title: Exploring Why Employees (Don't) Pay Attention to Cybersecurity)
- 2025-1622 Shields Activated – Strengthening Cyber Resilience for Small Businesses (no poster provided)
- 2025-1633 Digital Warrior (no poster provided)
- 2025-1642 Critical Infrastructure Cybersecurity Experiential Training Program
- 2025-1655 A Comprehensive Training Program for Advanced Cybersecurity in 5G Networks, ICS/CPS, and Beyond (no poster provided)
- 2025-1726 Driving Cybersecurity Excellence: Building Pathways To Reduce Labour and Skills Gaps
- 2025-1755 First Response for Cyber Threats (FRCT) - A Collaborative Cybersecurity Training Initiative
- 2025-1756 Preparing Canada's Workforce for the Future of Cybersecurity through Training and Academic Pathways

By Province

Alberta

- 2023-1485 Mobilizing Cybersecurity Regulation for Canada
- 2024-1305 Authentication for quantum-enabled secure communication (no poster provided)
- 2024-1346 Ostrich Accounting: Dotting i's and crossing t's with your head in the sand (no poster provided)
- 2024-1351 Protecting Democracy from Cyber Threats
- 2024-1356 Toward a Secure User-centric Green Credit Management System (no poster provided)
- 2024-1359 IncidentSync: Bridging IT and Law Enforcement

- 2024-1360 Adaptive Decision Defense System (ADDS): A Proactive Approach to Detecting and Mitigating Dual Denial of Decision Attacks in Critical Infrastructure
- 2024-1428 IntruderInsight: Elevating Cyber Attribution with AI Insights
- 2024-1469 CyberGuardian: Bridging the Cybersecurity Enforcement Training Gap
- 2025-1585 Prescriptive Analysis & Agentic Solutions for Disinformation & Digital Attacks (no poster provided)
- 2025-1610 Frontier Quantum-AI Cyber Defense: Pioneering Unprecedented Security Measures for Critical Infrastructure (Poster Title: Quantum-AI Security Framework for Critical Infrastructure and OT/IoT Systems)
- 2025-1689 Securing the Canadian software supply chain (Poster Title: Security Patch-Related regressions in Software Supply Chain)
- 2025-1690 Protecting Alberta & Nunavut HigherEd with Global Partnerships
- 2025-1753 Efficiency and Security of Unknown Group Order Cryptography
- 2025-1756 Preparing Canada's Workforce for the Future of Cybersecurity through Training and Academic Pathways
- 2025-1770 The Location Dragnet (no poster provided)

British Columbia

- 2024-1242 Accelerating Efforts to Secure Canada in an Era of Quantum
- 2024-1302 Fully Automated End-to-End Vulnerability Discovery and Repair with LLMs
- 2024-1322 ICS Security in the Age of Industry 4.0
- 2024-1386 Preserving Relationship Privacy in Large Networks
- 2024-1418 Novel methods for quantifying and improving privacy in machine learning
- 2025-1642 Critical Infrastructure Cybersecurity Experiential Training Program
- 2025-1643 Digital Twin Platform for Critical Infrastructure Cybersecurity Modeling and Assessment (Poster Title: Digital Twin Platform for Cybersecurity Critical Infrastructure)
- 2025-1657 Differential Programming and Fully-Homomorphic Encryption at the Edge
- 2025-1695 Vulnerabilities and Defences of Online Interactive Discussion Forums to Interference by Generative AI (Poster Title: Protecting Democratic Discourse from GenAIChatbots Posing as Humans)

- 2025-1759 Reliable and Explainable Malware Detection (Poster Title: Reliable Machine Learning for Android Malware Detection)

New Brunswick

- 2023-1497 Master in Cybersecurity Management (Poster Title: Cybersecurity Management Master)
- 2023-1498 Post-Quantum Hardware Security Module (HSM) Migration Research Project (no poster provided)
- 2023-1519 AI-enabled vulnerability management (no poster provided)
- 2024-1365 Fortifying Cybersecurity: Early Ransomware Detection and Mitigation methods
- 2024-1433 Enterprise-scale Zero Trust Platform for Privacy-enhancing Smart Metering Services (no poster provided)

Newfoundland & Labrador

- 2024-1326 SCMS: Securing Critical Marine Systems (Poster Title: Marine Cybersecurity)
- 2024-1354 MCT: Marine Cybersecurity Training (Poster Title: Marine Cybersecurity)

Nova Scotia

- 2025-1703 AI-Driven IoT Threat Intelligence: Securing Smart Environments Across Zigbee, Z-Wave, Bluetooth, and Wi-Fi Networks (Poster Title: AI-Driven IoT Threat Intelligence)
- 2025-1726 Driving Cybersecurity Excellence: Building Pathways To Reduce Labour and Skills Gaps

Ontario

- 2023-1482 Next Generation User Fingerprinting for Fraud Detection and Prediction
- 2023-1486 CyberLab
- 2023-1487 Trustworthy AI-based Framework for Self-aware Drone-based Swarm Technologies (Poster Title: GPS Spoofing Detection Using Online Federated TinyML for UAV Swarms)
- 2023-1488 Transfer Fuzzing for Devices Without Firmware
- 2023-1489 Mitigating Security, Privacy, and Ethical Impacts in Driver Assistance Systems (no poster provided)
- 2023-1494 PASCAL (Poster Title: PASCALProject: Defending Canada's Infrastructure with Physics-Based Supply Chain Security)

- 2023-1495 Designing a Scalable and Performant Confidential Backup System (no poster provided)
- 2023-1521 ATLAS (no poster provided)
- 2023-1523 CMD-CT: Comprehensive MultiDisciplinary Cybersecurity Training (no poster provided)
- 2024-1261 Enabling secure outsourcing of sensitive data (Poster Title: Designing a scalable oblivious Database)
- 2024-1282 End-to-end Cyber-Security Solution for the Power Grid
- 2024-1288 Human-Centric Immersive Cybersecurity Training: Socio-Technical and Legal Implications of an Attack
- 2024-1338 Adaptive Defense Strategies for Advanced Driver-assistance Systems: A Game-theoretic Approach (no poster provided)
- 2024-1345 Secure Genomic Data Processing: Unleashing the Potential of Personalized Medicine (Poster Title: Secure Genomic Data Processing)
- 2024-1358 CRAFT: Cybersecure Robotics and Future Talent (no poster provided)
- 2024-1361 Enhancing Electric Vehicle Charging Infrastructure Cybersecurity Through Autonomous and Sustainable AI
- 2024-1375 Security Awareness Training through Online Social Learning - "From Phishing through Smishing to Vishing" (Poster Title: Phishing, Smishing, Vishing)
- 2024-1381 Adaptive AI Firewall Specializing in the Protection of AI Models, Critical Infrastructure, Systems, and Agents
- 2024-1409 Transformative Adversaries: Leveraging Generative Pretrained Transformers (GPTs) for the Development of Next-Generation Metamorphic Malware Engines (no poster provided)
- 2024-1439 Privacy Assurance for Canadian Children: A Safe and Secure Framework for Large Language Models (Poster Title: A Human-Centric Framework for Managing Children's Privacy in Large Language Model Platforms)
- 2024-1454 Revolutionizing Personal Cyber Security with AI-driven Insights (no poster provided)
- 2024-1470 Ensuring Mission-Critical Security: Coordination of Autonomous Drone Groups with Security-Aware Decision Making
- 2025-1541 May We Have Your Attention Please? Exploring How Employee Attention Influences Cybersecurity Behaviour (Poster Title: Exploring Why Employees (Don't) Pay Attention to Cybersecurity)

- 2025-1548 Secure Healthcare Data Federation through Generative Access Control
- 2025-1601 Self-Healing AI Security via Autonomous Patch Generation & LLM Autovaccination
- 2025-1622 Shields Activated – Strengthening Cyber Resilience for Small Businesses (no poster provided)
- 2025-1630 Cyber-Synthetic Risk: A Generative Multi-Agent Approach to Forecasting Advanced Cyberattack Impacts on Enterprise Ecosystems
- 2025-1633 Digital Warrior (no poster provided)
- 2025-1650 Securing LLM Agents Against Malicious or Vulnerable Tools (Poster Title: Securing AI Agents Against Malicious or Vulnerable Tools)
- 2025-1660 MATSEC: Materials-based Cybersecurity in Electronics (no poster provided)
- 2025-1707 Cyber Resilient Battery Management System with secure Bi-directional Power Flow for Connected Vehicles
- 2025-1721 Threat Modelling and Mitigation of human-factors based exploits in advanced driver assistance systems
- 2025-1755 First Response for Cyber Threats (FRCT) - A Collaborative Cybersecurity Training Initiative
- 2025-1778 Post Quantum Resilience of Cyber-Physical Power Systems

Quebec

- 2023-1491 Hybrid Master's Program in Cybersecurity Analytics
- 2023-1492 Cybersécurité de l'identité numérique (Poster Title: Automatic Generation of Decentralized SSI Architectures)
- 2023-1493 Cloud Security Training Program (Micro-credential) (no poster provided)
- 2023-1496 Building cyber resilient and secure 5G networks through automation and AI
- 2023-1797 De la formation à la cyberstart-up innovante (no poster provided)
- 2024-1263 Évaluation de la cybersécurité de modèles prédéploiement de systèmes industriels (Poster Title: Cybersecurity Assessment of Pre-deployment Models of Industrial Systems)
- 2024-1301 Combatting Cyber Influence Operations in Online Social Media (no poster provided)
- 2024-1308 Securing the Metaverse with Blockchain and Continuous Authentication Methods (Poster Title: Securing the Metaverse with Multimodal Access Control and Authentication Methods)

- 2024-1372 C1R3 Commercialization (Poster Title: CitizenOne)
- 2024-1423 Formation pour une cybersécurité proactive et interdisciplinaire en entreprise (Poster Title: Parcours Cyber Action: Cybersecurity Training for SMEs)
- 2024-1458 Boosting the Cyber-Resilience of Microgrids within Future Energy Critical Infrastructures
- 2025-1584 Cybersecurity, Resilience, and Trustworthiness of Networked Critical Infrastructure and Autonomous Advanced Air Mobility (AAM) Assets Against Malicious Adversary Cyber-Attacks (Poster Title: Cybersecurity of Autonomous and Advanced/Urban/Electrified Urban Air Mobility (AAM/UAM/EAM))
- 2025-1647 CYBERDEFENSE AI Go-To-Market 2025-2027
- 2025-1649 Securing Agentic AI Systems Across the Development and Operations Lifecycle
- 2025-1655 A Comprehensive Training Program for Advanced Cybersecurity in 5G Networks, ICS/CPS, and Beyond (no poster provided)
- 2025-1663 Zero-Knowledge Threat Detection and Risk Assessment in Aerospace and Orbital Infrastructures

Saskatchewan

- 2023-1499 The run-time security of Android Automotive infotainment system (no poster provided)

By Funding Stream

Commercialization

- 2023-1494 PASCAL (Poster Title: PASCALProject: Defending Canada's Infrastructure with Physics-Based Supply Chain Security)
- 2024-1372 C1R3 Commercialization (Poster Title: CitizenOne)
- 2024-1469 CyberGuardian: Bridging the Cybersecurity Enforcement Training Gap
- 2025-1647 CYBERDEFENSE AI Go-To-Market 2025-2027

Research and Development

- 2023-1482 Next Generation User Fingerprinting for Fraud Detection and Prediction
- 2023-1487 Trustworthy AI-based Framework for Self-aware Drone-based Swarm Technologies (Poster Title: GPS Spoofing Detection Using Online Federated TinyML for UAV Swarms)

- 2023-1488 Transfer Fuzzing for Devices Without Firmware
- 2023-1489 Mitigating Security, Privacy, and Ethical Impacts in Driver Assistance Systems (no poster provided)
- 2023-1492 Cybersécurité de l'identité numérique (Poster Title: Automatic Generation of Decentralized SSI Architectures)
- 2023-1495 Designing a Scalable and Performant Confidential Backup System (no poster provided)
- 2023-1496 Building cyber resilient and secure 5G networks through automation and AI
- 2023-1498 Post-Quantum Hardware Security Module (HSM) Migration Research Project (no poster provided)
- 2023-1499 The run-time security of Android Automotive infotainment system (no poster provided)
- 2023-1519 AI-enabled vulnerability management (no poster provided)
- 2023-1521 ATLAS (no poster provided)
- 2024-1261 Enabling secure outsourcing of sensitive data (Poster Title: Designing a scalable oblivious Database)
- 2024-1263 Évaluation de la cybersécurité de modèles prédéploiement de systèmes industriels (Poster Title: Cybersecurity Assessment of Pre-deployment Models of Industrial Systems)
- 2024-1282 End-to-end Cyber-Security Solution for the Power Grid
- 2024-1301 Combatting Cyber Influence Operations in Online Social Media (no poster provided)
- 2024-1302 Fully Automated End-to-End Vulnerability Discovery and Repair with LLMs
- 2024-1305 Authentication for quantum-enabled secure communication (no poster provided)
- 2024-1308 Securing the Metaverse with Blockchain and Continuous Authentication Methods (Poster Title: Securing the Metaverse with Multimodal Access Control and Authentication Methods)
- 2024-1322 ICS Security in the Age of Industry 4.0
- 2024-1326 SCMS: Securing Critical Marine Systems (Poster Title: Marine Cybersecurity)
- 2024-1338 Adaptive Defense Strategies for Advanced Driver-assistance Systems: A Game-theoretic Approach (no poster provided)
- 2024-1345 Secure Genomic Data Processing: Unleashing the Potential of Personalized Medicine (Poster Title: Secure Genomic Data Processing)
- 2024-1346 Ostrich Accounting: Dotting i's and crossing t's with your head in the sand (no poster provided)
- 2024-1351 Protecting Democracy from Cyber Threats

- 2024-1356 Toward a Secure User-centric Green Credit Management System (no poster provided)
- 2024-1360 Adaptive Decision Defense System (ADDS): A Proactive Approach to Detecting and Mitigating Dual Denial of Decision Attacks in Critical Infrastructure
- 2024-1361 Enhancing Electric Vehicle Charging Infrastructure Cybersecurity Through Autonomous and Sustainable AI
- 2024-1365 Fortifying Cybersecurity: Early Ransomware Detection and Mitigation methods
- 2024-1375 Security Awareness Training through Online Social Learning - "From Phishing through Smishing to Vishing" (Poster Title: Phishing, Smishing, Vishing)
- 2024-1381 Adaptive AI Firewall Specializing in the Protection of AI Models, Critical Infrastructure, Systems, and Agents
- 2024-1386 Preserving Relationship Privacy in Large Networks
- 2024-1409 Transformative Adversaries: Leveraging Generative Pretrained Transformers (GPTs) for the Development of Next-Generation Metamorphic Malware Engines (no poster provided)
- 2024-1418 Novel methods for quantifying and improving privacy in machine learning
- 2024-1428 IntruderInsight: Elevating Cyber Attribution with AI Insights
- 2024-1433 Enterprise-scale Zero Trust Platform for Privacy-enhancing Smart Metering Services (no poster provided)
- 2024-1439 Privacy Assurance for Canadian Children: A Safe and Secure Framework for Large Language Models (Poster Title: A Human-Centric Framework for Managing Children's Privacy in Large Language Model Platforms)
- 2024-1454 Revolutionizing Personal Cyber Security with AI-driven Insights (no poster provided)
- 2024-1458 Boosting the Cyber-Resilience of Microgrids within Future Energy Critical Infrastructures
- 2024-1470 Ensuring Mission-Critical Security: Coordination of Autonomous Drone Groups with Security-Aware Decision Making
- 2025-1541 May We Have Your Attention Please? Exploring How Employee Attention Influences Cybersecurity Behaviour (Poster Title: Exploring Why Employees (Don't) Pay Attention to Cybersecurity)

- 2025-1548 Secure Healthcare Data Federation through Generative Access Control
- 2025-1584 Cybersecurity, Resilience, and Trustworthiness of Networked Critical Infrastructure and Autonomous Advanced Air Mobility (AAM) Assets Against Malicious Adversary Cyber-Attacks (Poster Title: Cybersecurity of Autonomous and Advanced/Urban/Electrified Urban Air Mobility (AAM/UAM/EAM))
- 2025-1585 Prescriptive Analysis & Agentic Solutions for Disinformation & Digital Attacks (no poster provided)
- 2025-1601 Self-Healing AI Security via Autonomous Patch Generation & LLM Autovaccination
- 2025-1610 Frontier Quantum-AI Cyber Defense: Pioneering Unprecedented Security Measures for Critical Infrastructure (Poster Title: Quantum-AI Security Framework for Critical Infrastructure and OT/IoT Systems)
- 2025-1630 Cyber-Synthetic Risk: A Generative Multi-Agent Approach to Forecasting Advanced Cyberattack Impacts on Enterprise Ecosystems
- 2025-1633 Digital Warrior (no poster provided)
- 2025-1643 Digital Twin Platform for Critical Infrastructure Cybersecurity Modeling and Assessment (Poster Title: Digital Twin Platform for Cybersecurity Critical Infrastructure)
- 2025-1649 Securing Agentic AI Systems Across the Development and Operations Lifecycle
- 2025-1650 Securing LLM Agents Against Malicious or Vulnerable Tools (Poster Title: Securing AI Agents Against Malicious or Vulnerable Tools)
- 2025-1657 Differential Programming and Fully-Homomorphic Encryption at the Edge
- 2025-1660 MATSEC: Materials-based Cybersecurity in Electronics (no poster provided)
- 2025-1663 Zero-Knowledge Threat Detection and Risk Assessment in Aerospace and Orbital Infrastructures
- 2025-1689 Securing the Canadian software supply chain (Poster Title: Security Patch-Related regressions in Software Supply Chain)
- 2025-1690 Protecting Alberta & Nunavut HigherEd with Global Partnerships
- 2025-1695 Vulnerabilities and Defences of Online Interactive Discussion Forums to Interference by Generative AI (Poster Title: Protecting Democratic Discourse from GenAIChatbots Posing as Humans)

- 2025-1703 AI-Driven IoT Threat Intelligence: Securing Smart Environments Across Zigbee, Z-Wave, Bluetooth, and Wi-Fi Networks (Poster Title: AI-Driven IoT Threat Intelligence)
- 2025-1707 Cyber Resilient Battery Management System with secure Bi-directional Power Flow for Connected Vehicles
- 2025-1721 Threat Modelling and Mitigation of human-factors based exploits in advanced driver assistance systems
- 2025-1753 Efficiency and Security of Unknown Group Order Cryptography
- 2025-1759 Reliable and Explainable Malware Detection (Poster Title: Reliable Machine Learning for Android Malware Detection)
- 2025-1770 The Location Dragnet (no poster provided)
- 2025-1778 Post Quantum Resilience of Cyber-Physical Power Systems

Training

- 2023-1485 Mobilizing Cybersecurity Regulation for Canada
- 2023-1486 CyberLab
- 2023-1491 Hybrid Master's Program in Cybersecurity Analytics
- 2023-1493 Cloud Security Training Program (Micro-credential) (no poster provided)
- 2023-1497 Master in Cybersecurity Management (Poster Title: Cybersecurity Management Master)
- 2023-1523 CMD-CT: Comprehensive MultiDisciplinary Cybersecurity Training (no poster provided)
- 2023-1797 De la formation à la cyberstart-up innovante (no poster provided)
- 2024-1242 Accelerating Efforts to Secure Canada in an Era of Quantum
- 2024-1288 Human-Centric Immersive Cybersecurity Training: Socio-Technical and Legal Implications of an Attack
- 2024-1354 MCT: Marine Cybersecurity Training (Poster Title: Marine Cybersecurity)
- 2024-1358 CRAFT: Cybersecure Robotics and Future Talent (no poster provided)
- 2024-1359 IncidentSync: Bridging IT and Law Enforcement
- 2024-1423 Formation pour une cybersécurité proactive et interdisciplinaire en entreprise (Poster Title: Parcours Cyber Action: Cybersecurity Training for SMEs)

- 2025-1622 Shields Activated – Strengthening Cyber Resilience for Small Businesses (no poster provided)
- 2025-1642 Critical Infrastructure Cybersecurity Experiential Training Program
- 2025-1655 A Comprehensive Training Program for Advanced Cybersecurity in 5G Networks, ICS/CPS, and Beyond (no poster provided)
- 2025-1726 Driving Cybersecurity Excellence: Building Pathways To Reduce Labour and Skills Gaps
- 2025-1755 First Response for Cyber Threats (FRCT) - A Collaborative Cybersecurity Training Initiative
- 2025-1756 Preparing Canada's Workforce for the Future of Cybersecurity through Training and Academic Pathways

By Focus Area

Commercialization Projects

Technology / product / service in the area of software security

- 2025-1647 CYBERDEFENSE AI Go-To-Market 2025-2027

Technology / product / service in the area of critical infrastructure protection

- 2023-1494 PASCAL (Poster Title: PASCALProject: Defending Canada's Infrastructure with Physics-Based Supply Chain Security)

Technology / product / service in the area of human elements in cybersecurity

- 2024-1469 CyberGuardian: Bridging the Cybersecurity Enforcement Training Gap

Technology / product / service in the area of privacy and privacy enhancing technologies

- 2024-1372 C1R3 Commercialization (Poster Title: CitizenOne)

Research and Development Projects

Science / Technology relating to Critical Infrastructure Protection

- 2023-1487 Trustworthy AI-based Framework for Self-aware Drone-based Swarm Technologies (Poster Title: GPS Spoofing Detection Using Online Federated TinyML for UAV Swarms)
- 2023-1489 Mitigating Security, Privacy, and Ethical Impacts in Driver Assistance Systems (no poster provided)

- 2023-1492 Cybersécurité de l'identité numérique (Poster Title: Automatic Generation of Decentralized SSI Architectures)
- 2023-1499 The run-time security of Android Automotive infotainment system (no poster provided)
- 2024-1263 Évaluation de la cybersécurité de modèles prédéploiement de systèmes industriels (Poster Title: Cybersecurity Assessment of Pre-deployment Models of Industrial Systems)
- 2024-1282 End-to-end Cyber-Security Solution for the Power Grid
- 2024-1322 ICS Security in the Age of Industry 4.0
- 2024-1326 SCMS: Securing Critical Marine Systems (Poster Title: Marine Cybersecurity)
- 2024-1345 Secure Genomic Data Processing: Unleashing the Potential of Personalized Medicine (Poster Title: Secure Genomic Data Processing)
- 2024-1360 Adaptive Decision Defense System (ADDS): A Proactive Approach to Detecting and Mitigating Dual Denial of Decision Attacks in Critical Infrastructure
- 2024-1361 Enhancing Electric Vehicle Charging Infrastructure Cybersecurity Through Autonomous and Sustainable AI
- 2024-1365 Fortifying Cybersecurity: Early Ransomware Detection and Mitigation methods
- 2024-1381 Adaptive AI Firewall Specializing in the Protection of AI Models, Critical Infrastructure, Systems, and Agents
- 2024-1428 IntruderInsight: Elevating Cyber Attribution with AI Insights
- 2024-1433 Enterprise-scale Zero Trust Platform for Privacy-enhancing Smart Metering Services (no poster provided)
- 2024-1458 Boosting the Cyber-Resilience of Microgrids within Future Energy Critical Infrastructures
- 2025-1584 Cybersecurity, Resilience, and Trustworthiness of Networked Critical Infrastructure and Autonomous Advanced Air Mobility (AAM) Assets Against Malicious Adversary Cyber-Attacks (Poster Title: Cybersecurity of Autonomous and Advanced/Urban/Electrified Urban Air Mobility (AAM/UAM/EAM))
- 2025-1601 Self-Healing AI Security via Autonomous Patch Generation & LLM Autovaccination
- 2025-1643 Digital Twin Platform for Critical Infrastructure Cybersecurity Modeling and Assessment (Poster Title: Digital Twin Platform for Cybersecurity Critical Infrastructure)
- 2025-1660 MATSEC: Materials-based Cybersecurity in Electronics (no poster provided)

- 2025-1663 Zero-Knowledge Threat Detection and Risk Assessment in Aerospace and Orbital Infrastructures

Science / Technology relating to Human-Centric Cybersecurity

- 2023-1482 Next Generation User Fingerprinting for Fraud Detection and Prediction
- 2024-1301 Combatting Cyber Influence Operations in Online Social Media (no poster provided)
- 2024-1351 Protecting Democracy from Cyber Threats
- 2024-1375 Security Awareness Training through Online Social Learning - "From Phishing through Smishing to Vishing" (Poster Title: Phishing, Smishing, Vishing)
- 2024-1454 Revolutionizing Personal Cyber Security with AI-driven Insights (no poster provided)
- 2025-1541 May We Have Your Attention Please? Exploring How Employee Attention Influences Cybersecurity Behaviour (Poster Title: Exploring Why Employees (Don't) Pay Attention to Cybersecurity)
- 2025-1585 Prescriptive Analysis & Agentic Solutions for Disinformation & Digital Attacks (no poster provided)
- 2025-1633 Digital Warrior (no poster provided)
- 2025-1721 Threat Modelling and Mitigation of human-factors based exploits in advanced driver assistance systems

Science / Technology relating to Network Security

- 2023-1496 Building cyber resilient and secure 5G networks through automation and AI
- 2023-1498 Post-Quantum Hardware Security Module (HSM) Migration Research Project (no poster provided)
- 2023-1519 AI-enabled vulnerability management (no poster provided)
- 2023-1521 ATLAS (no poster provided)
- 2024-1302 Fully Automated End-to-End Vulnerability Discovery and Repair with LLMs
- 2024-1305 Authentication for quantum-enabled secure communication (no poster provided)
- 2024-1356 Toward a Secure User-centric Green Credit Management System (no poster provided)
- 2024-1409 Transformative Adversaries: Leveraging Generative Pretrained Transformers (GPTs) for the Development of Next-Generation Metamorphic Malware Engines (no poster provided)

- 2024-1470 Ensuring Mission-Critical Security: Coordination of Autonomous Drone Groups with Security-Aware Decision Making
- 2025-1690 Protecting Alberta & Nunavut HigherEd with Global Partnerships
- 2025-1703 AI-Driven IoT Threat Intelligence: Securing Smart Environments Across Zigbee, Z-Wave, Bluetooth, and Wi-Fi Networks (Poster Title: AI-Driven IoT Threat Intelligence)

Science / Technology relating to Privacy Protection

- 2024-1261 Enabling secure outsourcing of sensitive data (Poster Title: Designing a scalable oblivious Database)
- 2024-1308 Securing the Metaverse with Blockchain and Continuous Authentication Methods (Poster Title: Securing the Metaverse with Multimodal Access Control and Authentication Methods)
- 2024-1346 Ostrich Accounting: Dotting i's and crossing t's with your head in the sand (no poster provided)
- 2024-1386 Preserving Relationship Privacy in Large Networks
- 2024-1418 Novel methods for quantifying and improving privacy in machine learning
- 2024-1439 Privacy Assurance for Canadian Children: A Safe and Secure Framework for Large Language Models (Poster Title: A Human-Centric Framework for Managing Children's Privacy in Large Language Model Platforms)
- 2025-1657 Differential Programming and Fully-Homomorphic Encryption at the Edge
- 2025-1753 Efficiency and Security of Unknown Group Order Cryptography
- 2025-1770 The Location Dragnet (no poster provided)

Science / Technology relating to Software Security

- 2023-1488 Transfer Fuzzing for Devices Without Firmware
- 2023-1495 Designing a Scalable and Performant Confidential Backup System (no poster provided)
- 2024-1338 Adaptive Defense Strategies for Advanced Driver-assistance Systems: A Game-theoretic Approach (no poster provided)
- 2025-1548 Secure Healthcare Data Federation through Generative Access Control
- 2025-1649 Securing Agentic AI Systems Across the Development and Operations Lifecycle
- 2025-1650 Securing LLM Agents Against Malicious or Vulnerable Tools (Poster Title: Securing AI Agents Against Malicious or Vulnerable Tools)

- 2025-1689 Securing the Canadian software supply chain (Poster Title: Security Patch-Related regressions in Software Supply Chain)
- 2025-1759 Reliable and Explainable Malware Detection (Poster Title: Reliable Machine Learning for Android Malware Detection)

Skills and talent development projects

Cyber Security Awareness

- 2023-1523 CMD-CT: Comprehensive MultiDisciplinary Cybersecurity Training (no poster provided)
- 2024-1242 Accelerating Efforts to Secure Canada in an Era of Quantum
- 2024-1423 Formation pour une cybersécurité proactive et interdisciplinaire en entreprise (Poster Title: Parcours Cyber Action: Cybersecurity Training for SMEs)

Professional

- 2023-1485 Mobilizing Cybersecurity Regulation for Canada
- 2023-1493 Cloud Security Training Program (Micro-credential) (no poster provided)
- 2023-1797 De la formation à la cyberstart-up innovante (no poster provided)
- 2024-1288 Human-Centric Immersive Cybersecurity Training: Socio-Technical and Legal Implications of an Attack
- 2024-1354 MCT: Marine Cybersecurity Training (Poster Title: Marine Cybersecurity)

Training Capacity

- 2024-1358 CRAFT: Cybersecure Robotics and Future Talent (no poster provided)
- 2025-1642 Critical Infrastructure Cybersecurity Experiential Training Program
- 2025-1695 Vulnerabilities and Defences of Online Interactive Discussion Forums to Interference by Generative AI (Poster Title: Protecting Democratic Discourse from GenAIChatbots Posing as Humans)

Training leading to certification

- 2024-1359 IncidentSync: Bridging IT and Law Enforcement
- 2025-1610 Frontier Quantum-AI Cyber Defense: Pioneering Unprecedented Security Measures for Critical Infrastructure (Poster Title:

Quantum-AI Security Framework for Critical Infrastructure and OT/IoT Systems)

- 2025-1630 Cyber-Synthetic Risk: A Generative Multi-Agent Approach to Forecasting Advanced Cyberattack Impacts on Enterprise Ecosystems
- 2025-1655 A Comprehensive Training Program for Advanced Cybersecurity in 5G Networks, ICS/CPS, and Beyond (no poster provided)
- 2025-1726 Driving Cybersecurity Excellence: Building Pathways To Reduce Labour and Skills Gaps

Upskilling

- 2023-1486 CyberLab
- 2025-1622 Shields Activated – Strengthening Cyber Resilience for Small Businesses (no poster provided)
- 2025-1707 Cyber Resilient Battery Management System with secure Bi-directional Power Flow for Connected Vehicles
- 2025-1755 First Response for Cyber Threats (FRCT) - A Collaborative Cybersecurity Training Initiative
- 2025-1756 Preparing Canada's Workforce for the Future of Cybersecurity through Training and Academic Pathways
- 2025-1778 Post Quantum Resilience of Cyber-Physical Power Systems

Graduate

- 2023-1491 Hybrid Master's Program in Cybersecurity Analytics
- 2023-1497 Master in Cybersecurity Management (Poster Title: Cybersecurity Management Master)

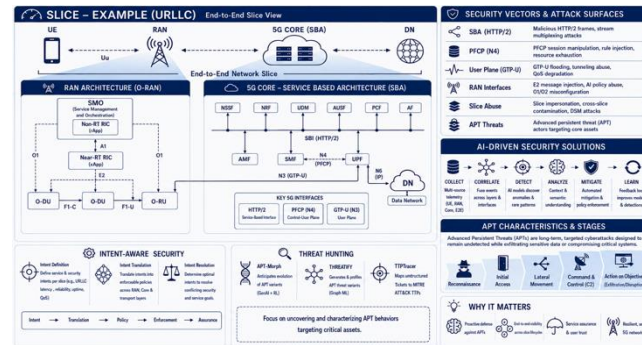
Critical Infrastructure





Project Description

- Mobile network evolution through 5G enabled flexible service delivery, but introduced new attack surfaces that manual security can no longer handle.
- Our project aims to harden 5G networks through threat hunting and anomaly detection on network slicing, protocol-level attack detection, and O-RAN security.
- We deliver automated, closed-loop AI-based security mechanisms protecting mobile operators' availability, reliability, and users' Quality of Service (QoS).
- Team:** Chadi Assi, Mourad Debbabi, Suryadip Majumdar, Lingyu Wang, Abdelhak Bentaleb & Carol Fung, based at the Computer Security Lab, Gina Cody School of Engineering, Concordia University.



Current Progress

- 8+ AI-powered tools delivered, including ThreatScout, THREATIFY, APTMorph, FlowGuardian & TIPTTracer (threat hunting), Inter-Slice Defender (DSM attacks), 5GShield (HTTP/2), RAN-GUARD & BTS-Band (O-RAN), and a QoS-based anomaly detection solution, collectively securing 5G network slicing and O-RAN infrastructure.
- GSMA recognition: our novel QoS-based attack discovery led to official updates to GSMA FS.30 & FS.31, adding attack descriptions and security controls now adopted globally.
- 5+ patents filed covering threat hunting, QoS anomaly detection & mitigation, and user data theft prevention.
- 20+ publications in IEEE S&P, IEEE TIFS, IEEE TMC, IEEE TNSM, ACM WISEC, IEEE CNS, CNSM & Elsevier, earning 3 international awards and a public MITRE ATT&CK dataset on IEEE Xplore.
- Expanding frontiers: fuzzing, trust management & intent-based networking for autonomous, self-healing 5G security.

Budget & Method

- Budget:** \$1.5 million NCC contribution matched with \$1.5 million from partners (+ ~300K from PROMPT, and in-kind) reflecting a strong academia-industry co-investment in Canadian cybersecurity innovation.
- Collaboration:** Weekly team meetings and quarterly steering committee reviews ensure continuous alignment across all partner institutions.
- Standards Engagement:** Active participation in 3GPP and GSMA working groups, ensuring research is grounded in and contributes back to global 5G security standards.
- Validation:** Research findings validated through proof-of-concept (PoC) implementations deployed and tested in realistic 5G network environments.



This project is made possible with the support of the National Cybersecurity Consortium and the Government of Canada (CSN).
Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RCC).

Acknowledgements

Project

Collaborators

- Ericsson:** Hyame Alameddine, Boubakr Nour, Amine Boukhtouta, Luis Suarez, Makan Pourzandi.
- Concordia University:** Chadi Assi, Mourad Debbabi, Abdelhak Bentaleb, Carol Fung, Lingyu Wang.
- University of Waterloo:** Raouf Boutaba.
- University of Manitoba:** Azadeh Tabiban.



Future Exploration

- O-RAN Testbed Acquisition:** Expanding to a physical O-RAN testbed for real-world validation of security solutions, moving from proof-of-concept to full-scale deployment.
- Advanced O-RAN Security:** Security intent translation into enforceable policies, resolution of conflicting intent-based policies, and contextual planning during adverse cybersecurity events.
- Automated Threat Hunting & CTI:** Automated cyber threat intelligence (CTI) extraction, evolving defense mechanisms, proactive vulnerability detection, and fully automated security operations.
- Trust & Orchestration:** Trusted orchestration frameworks and adaptive threat modeling for flexible, secure Telco Cloud Native applications.
- Intent-Based Networking & Security Posture:** Closing the loop between security posture evaluation and autonomous, self-healing 5G network protection through intent-based networking.



Project Description

Context & Environment

- Rising Threats: Targeted cyberattacks on critical infrastructure, especially ICS
- Emulation Platform: Cyber Range integrated with real hardware for faithful ICS simulation
- AI & ICS Integration: Dynamic evaluation using AI-based threat modeling
- Academic-Industry Collaboration: Consortium led by University of Sherbrooke, supported by NCC and Government of Canada

Objectives

- O1. Develop a robust cybersecurity assessment methodology prior to deployment
- O2. Improve the cybersecurity practices of ICS integrators
- O3. Automate the detection of successful attacks based on logging
- O4. Produce recommendations based on the results of ICS penetration tests

Project Collaborators

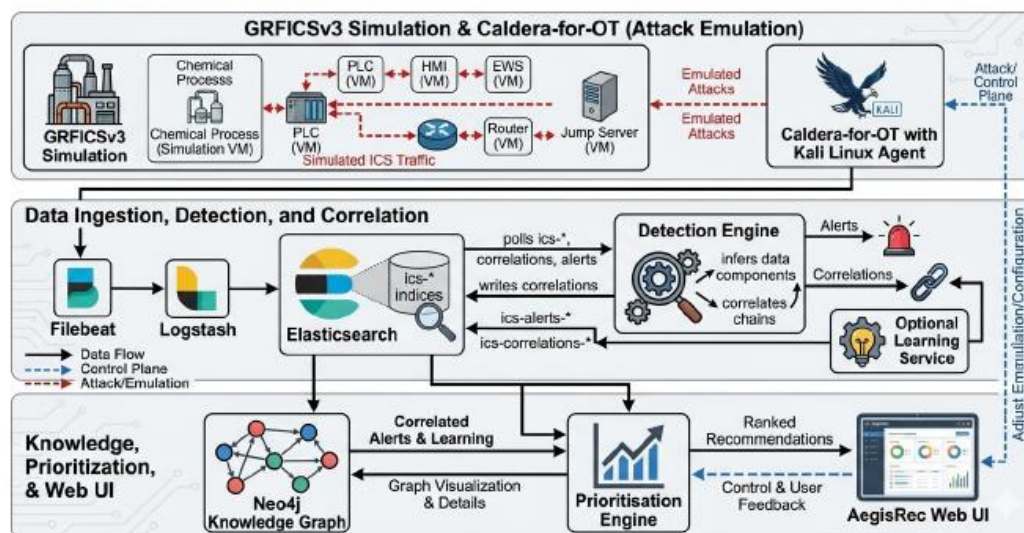
Beneficiary

- Université de Sherbrooke

Partners

- ICS infrastructure : Productique Québec
- ICS integrator : Centris Technologies
- AI Pentesting : NeverHack

Current Progress & Method



Budget

Total budget :	810 800 \$
NCC grant :	480 000 \$
Matching :	330 800 \$

Future Exploration

- Extend the emulation environment to a variety of ICS technologies
- Document cybersecurity best practices for ICS integrators
- Explore LLM usage as a recommendation system



Acknowledgements

This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (GCN).
Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (NCC).
Add any other acknowledgements as appropriate.

End-to-End Cyber-Security Solution for the Power Grid

Pirathayini Srikantha, York University

Project Description

Climate change concerns have spurred the proliferation of independent power producers (e.g. renewables) in the electric grid along with significant increase in power demands due to the electrification of fossil-fuel based technologies (e.g. transportation). Grid communications are critical for effectively coordinating the evolving grid. However, as these utilize open protocols, traverse the public domain (e.g. internet) and utilize easily accessible physical medium (e.g. wireless), stealthy cyber attacks can leverage on existing vulnerabilities in these to infiltrate and destabilize grid operations.

We propose an end-to-end cyber security solution that leverages on the natural interdependencies of the cyber and physical domains of the electric grid to actively secure, detect and mitigate natural and adversarial perturbations in grid communications. Specifically, lightweight encryption protocols tailored for the unique attributes of grid communications and optional embedded systems based interfaces will be designed so that common grid computations can be performed in the cipher domain. Then, data-driven and physics-based approaches will be leveraged to detect anomalies in grid communications that will then be actively corrected via generative techniques.

A prototype of the proposed algorithms will be implemented in standard IEEE benchmark systems along with software libraries.

Project Collaborators

Cistel Technology
Siemens Inc.
IESO
Dalhousie University
Carleton University

Budget & Method

Budget (over 3 years):

- NCC's contribution: \$300,000
- Cash contribution by Cistel: \$60,000
- In-kind contributions by all industry collaborators: \$244,760
- Budget will be used to fund 2 Phds, 2 Masters and 1 Research Associate

Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).



ICS Security in the Age of Industry 4.0

Aastha Mehta* (PL), Karthik Pattabiraman (Co-PI), Gargi Mitra (Group member)
The University of British Columbia, *Email: aasthakm@cs.ubc.ca



Project Description

Denial of Service (DoS) attacks on Industrial Control Systems (ICS)



Safety risks

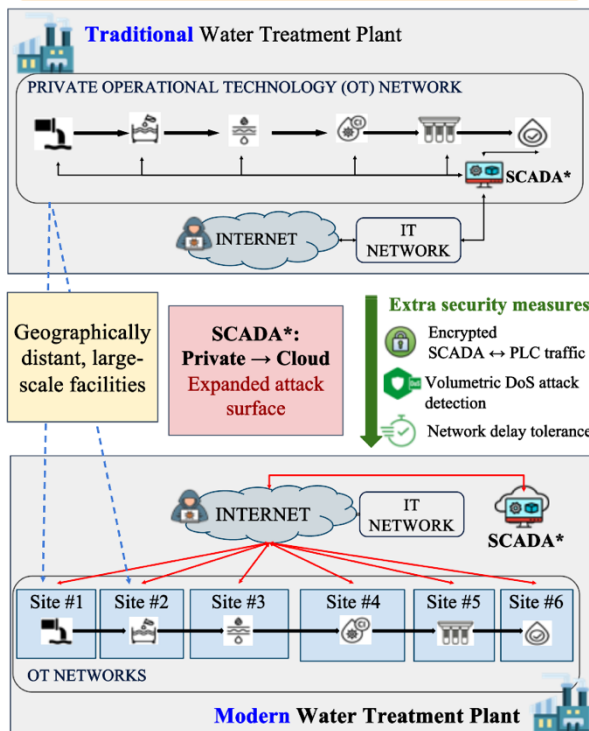


Civilian inconvenience



Financial losses

How can we detect and mitigate emerging DoS threats in modern ICS connected to the Internet?



*SCADA: Supervisory Control And Data Acquisition system

Budget & Method



Source: The National Cybersecurity Consortium (NCC)

Contribution: 500,000 CAD

Current and Past Team (non-PIs)

1. Gargi Mitra: Postdoctoral Fellow
2. Chanyuan Liu: Research Programmer
3. Kelly Hum: USRA Intern
4. Alain Zhiyanov: Past UG student (currently, Software Engineer Intern at Microsoft)

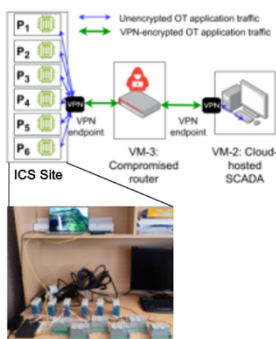


Method: Build testbed → Demonstrate novel DoS attacks on the testbed → Design efficient countermeasures

Current Progress

ICS-Sniper : A Novel Targeted DoS Attack on a Modern ICS

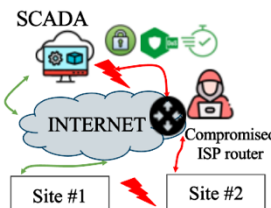
Contribution #1: Realistic testbed, mimicking a 6-stage water treatment plant



Schematic of our testbed.

P1-P6 : Stages of water treatment
Supports 2 comm. protocols,
configurable process variables

Contribution #2: Novel encrypted ICS traffic pattern analysis technique to identify time-critical packets



Loss of synchronization

Drops only a **small number** of **highly time-critical** packets

- Break encryption / see data / Know process details ✗
- See traffic metadata ✓

Future Exploration

Defensive Research Directions



Early attack detection

- Distinguishing between benign network delay and ICS-Sniper
- Proactive process-aware network delay monitoring



Attack prevention

- Traffic shaping across the network stack, with minimum latency and bandwidth overhead

Implementation and testing on our in-house testbed

Future directions : Evaluate real-world impact, **foster industry collaborations**

The Team



Aastha Mehta

Assistant Professor @UBC CS



Karthik Pattabiraman

Professor @UBC ECE

+ students and Postdoctoral researcher

Acknowledgments



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).



UNIVERSITY OF
CALGARY

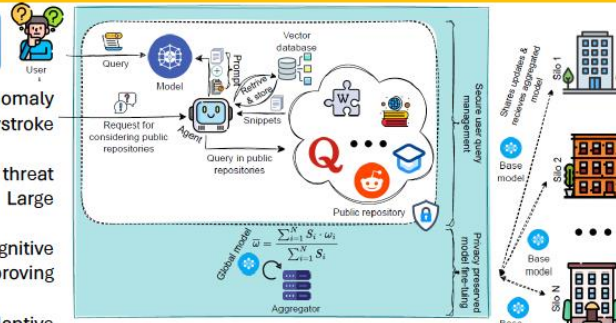
Adaptive Decision Defense System (ADDS): A Proactive Approach to Detecting and Mitigating Dual Denial of Decision Attacks in Critical Infrastructure

Hadis Karimipour, Anik Islam, Rubina Akter
Department of Electrical and Software Engineering,
University of Calgary
{hadis.karimipour, anik.islam, rubina.akter}@ucalgary.ca

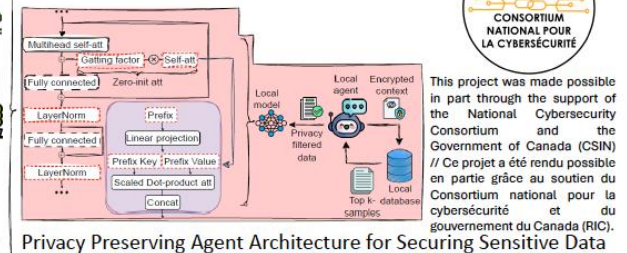


Project Description

- AI-Powered Threat Detection** — Develops a Behavioral Anomaly Analytics Engine using ML to detect insider threats through keystroke dynamics, communication patterns, and sentiment analysis.
- Real-Time Intelligence Integration** — Integrates live threat intelligence feeds with AI/NLP-driven anomaly detection and Large Language Models (LLMs) for advanced cybersecurity analysis.
- Human-AI Collaboration & Cognitive Support** — Builds Cognitive AI tools to monitor operator stress and fatigue in real time, improving decision-making during high-pressure cyber incidents.
- Zero Trust & Quantum-Ready Defense** — Establishes an adaptive Zero Trust network with post-quantum cryptography and an autonomous Cognitive Defense Architecture to counter evolving threats.



Acknowledgements



Privacy Preserving Agent Architecture for Securing Sensitive Data

Project Collaborators

This project brings together a team of esteemed researchers from leading Canadian institutions. Dr. Hadis Karimipour (Project Lead, University of Calgary) and Dr. Talal Halabi (Co-Lead, Laval University) guide the overall vision and execution. Contributing their expertise as investigators are Dr. Lorenzo De Carli, Dr. Benjamin Tan, and Dr. Rei Safavi-Naeini from the University of Calgary, alongside Dr. Fattane Zarrinkalam from the University of Guelph.

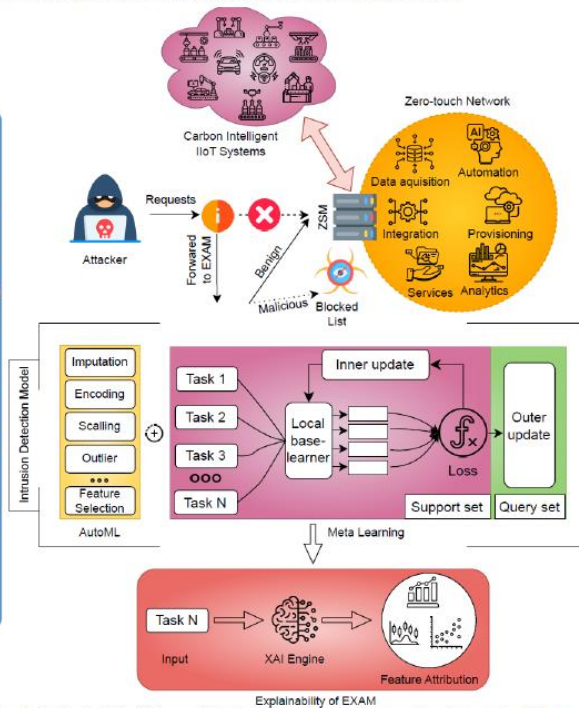
Budget & Method

The project is being executed through a strategic allocation of resources, focusing on two key components: human expertise and computational infrastructure. The allocated budget is utilized primarily for personnel support, including postdoctoral researchers (\$60,000/year) and PhD students (\$30,000/year). Additionally, a significant portion is invested in high-performance computing (HPC) systems, which are essential for processing large datasets and running complex simulations efficiently.

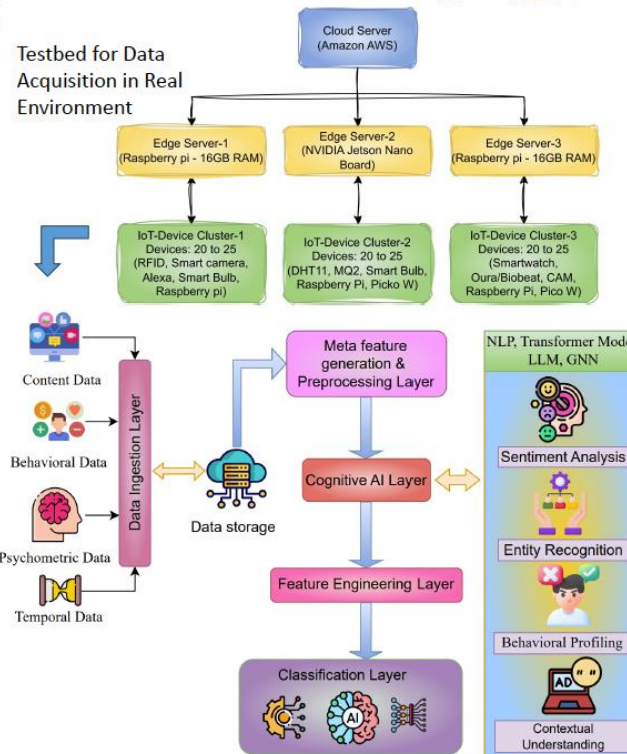
Future Exploration

Advance human-centric and future-resilient security through stress-aware UX, post-quantum IoT provisioning, and adversarial validation using GANs and LLMs by 2027.

Current Progress



Explainable AutoML-Driven Meta-Learning Scheme for Intrusion Prevention



Transformer based Hybrid Model for Insider Threat Detection

Boosting the Cyber-Resilience of Microgrids within Future Energy Critical Infrastructures

Mohsen Ghafouri, CONCORDIA UNIVERSITY

Project Description

With North America alone witnessing a growth rate of 13.5% from 2022 to 2030 in the MG sector and significant investments in grid modernization and renewables, enhancing the security and resilience of MGs is crucial.

Thus, we aim to address their major operational issues, including susceptibility to cyber-physical attacks, and improving survivability and recovery following successful attacks. To this end, first, a co-simulation cyber-physical testbed will be developed to generate various IT/OT data. Afterward, possible attack surfaces and vulnerabilities of MGs will be identified, and their associated risks and impacts will be investigated.

To enhance the survivability of MGs, this project will develop optimization-based frameworks for both the planning and operation phases. Next, attack detection and mitigation tools will be developed to counter threats. Finally, an optimization-based framework will be developed, based on the security and operation constraints, to successfully recover from cyber-attacks. These envisioned designs, algorithms, and tools will enhance the quality of energy delivery, significantly reducing the risk of blackouts and brownouts, e.g., only in Quebec a 20% decrease in outages is translated to an estimated \$200 million annually. Moreover, MGs are ideal for electrifying over 170 remote communities in Canada, provided these systems are secure and resilient.

Budget

- **Project Total - \$540,940.00**
- NCC Request - \$352,940.00
- In-Kind - \$28,000.00
- Cash - \$160,000.00

Collaborations

- RMDS Innovation Inc
- University of New Brunswick

Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).

Ensuring Mission-Critical Security: Coordination of Autonomous Drones Groups with Security-Aware Decision Making

Davide Spinello, University of Ottawa, davide.Spinello@uottawa.ca
Mohammad Pirani, University of Ottawa, mpirani@uottawa.ca

Project Description

Project Description

We study stealthy cyber-attacks in networks by analyzing the zero dynamics and by designing detection algorithms using system redundancies. We also develop optimal control strategies under uncertain, adversarial conditions.

Goals and Milestones

- Identify undetectable attacks via zero dynamics
- Develop detection methods using analytical and temporal redundancies
- Design optimal controllers based on adversarial threat distributions

Context

The project lies at the intersection of secure control and cyber-physical systems, with relevance to autonomous systems and critical infrastructure

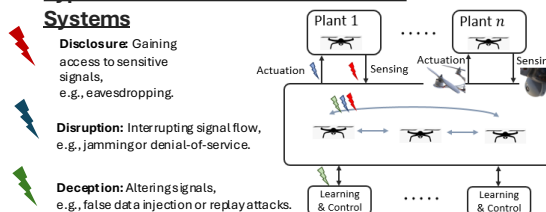
Methodology

Zero Dynamics Attacks and Defensive Control

We consider *zero dynamics attacks*—inputs $u(t)$ that leave the system output unchanged: $y(u, x, t) = y(0, x, t)$ (stealthy output unchanged)

- Attacker's Goal: find a strategy u that maximizes the system's utility function (i.e. energy-induced activity).
- Defender's Goal: find a strategy π that minimizes the system's utility function (conflicting goals on the same utility)
- Game-theoretic setup: it models adversarial attacks and optimal feedback defense in cyber-physical systems.

Types of Attacks in Network Control Systems



Budget

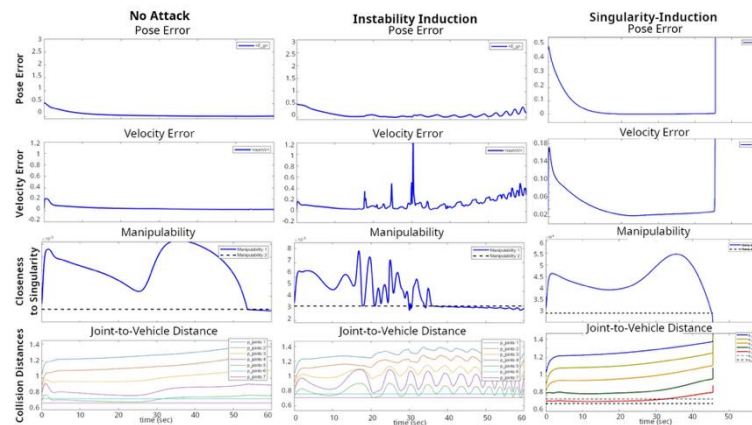
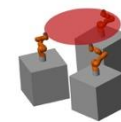
Funding sources:

- NCC grant (499k total, 50% to each academic partner)
- Quanser Inc. provides cash contributions in terms of engineering hours and software licenses for testing on their digital twin platform.
- DRDC-CORA provide funds to develop defense systems, with some theoretical background in common (HQP cross funded)

The expenses consist to salaries and bursaries for postdocs and graduate students, and related conference and publication costs.

Current Progress

- Intelligent Null-Space Attacks*: attacker model that injects low-energy inputs under stealth constraints, targeting five failure modes: singularity, self-collision, obstacle collision, instability, and deadlock.
- Stealthy failure in multiple modes* with bounded task-space deviation, highlighting *critical vulnerabilities* in redundant networks of robots.



Future Exploration: Two-Level Strategic Game

Module 1: Strategic Decision-Making

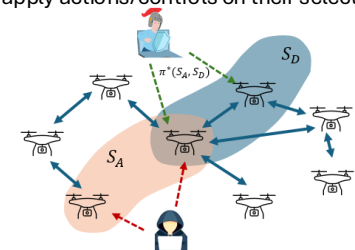
Define S_A and S_D as decision variables over nodes/edges for attacker and defender, respectively. The optimal strategies (in a game theoretical sense) are determined by

$$\min_{S_D} \max_{S_A} \|T(S_A, S_D)\|_{\mathcal{H}_\infty}$$

where $T(S_A, S_D)$ is the closed-loop transfer function of the system for selected attack/control locations.

Module 2: Strategic Control

Given the optimal strategies S_A, S_D , the attacker and defender apply actions/controls on their selected nodes



Project Collaborators

- Walter Lucia and Amr Youssef
{walter.lucia, amr.youssef}@concordia.ca
- Quanser Inc.



Acknowledgements

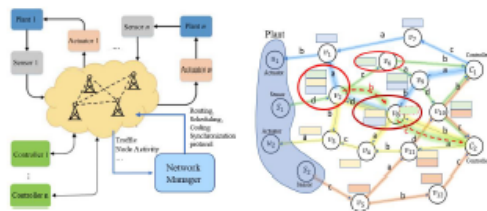
This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (DRDC-CORA). // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (DRDC-CORA).

Cybersecurity of Autonomous and Advanced/Urban/Electrified Urban Air Mobility (AAM/UAM/EAM)

K. Khorasani, Dept. of Electrical & Computer Eng., Concordia University, kash@ece.concordia.ca
(Drs. Saif (Windsor), Sepeluri (Manitoba), Marquez (Alberta)) & Humanitas and Vozwin Inc.

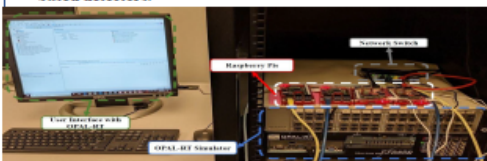
1 Cyber-Attack Detection, Isolation and Recovery for Multi-Agent Systems (MAS) and Advanced Air Mobility (AAM)

- Our objectives are to develop novel cybersecurity, fleet cyber readiness and resilient control methodologies to ensure 24/7-available MAS/AAM sustainability and survivability under presence of malicious cyberattacks and cyber-physical manipulations by adversaries. The research challenges are:
 - Agent Cybersecurity: to prevent, detect, isolate attacks from entry into MAS/AAM.
 - Infrastructure Cybersecurity: to protect the infrastructure equipment, devices and Integrated Platform Management System (IPMS), Positioning, Navigation, and Timing (PNT), among others from threats, and
 - Communication Security: to ensure trusted communications among fleet of MAS/AAM.
- Cyber-attack diagnosis and resilient recovery for MAS/AAM:
 - Machine learning-based methods
 - Model-based methods (adaptive observer)
 - Hybrid methods



3 Cyber-Attack and Fault Detection and Isolation

- We have studied the problem of cyber-attack and fault detection and isolation (CAFDI) for CPS under malicious deception cyber-attacks, such as covert attacks, zero dynamics attacks, replay attacks, and false data injection attacks.
- Two filters are designed on both the plant side and the command and control (C&C) side of CPS interconnected via not necessarily secure communication links.
- On the plant side UIO-based detectors are designed to generate residuals for detecting and isolating actuator cyber-attacks, sensor cyber-attacks, as well as actuator faults, and sensor faults while the adversary have a complete knowledge of the filters and UIO-based detectors.

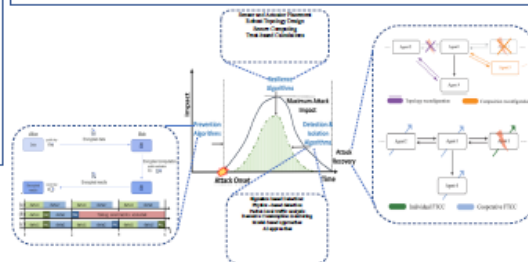


Acknowledgements

This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (GCN).
Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (GNC).

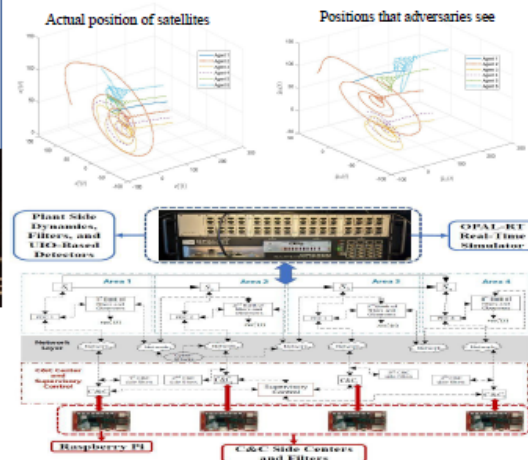
2 Cybersecurity of MAS/AAM/UAM: System Monitoring & Risk Mitigation Support

- Developing monitoring solutions for potential vulnerable assets for detecting presence of adversaries.
- Detectability analysis, and sensor placement strategies in case of major deficiencies in networked data have been provided.
- Developing Resilient Algorithms for Control, Estimation, and Optimization.
- Developing Passive and Active Detection Algorithms.
- Developing Recovery Guidelines and Automatic Reconfiguration Algorithms.



4 Privacy Preserving Control for AAM/UAM and Autonomous Systems

- A unique coding scheme is developed and designed for each AAM/UAM/autonomous system so that adversaries require discovering all the utilized transformations to disclose information of the entire fleet.
- To preserve the privacy of autonomous system/AAM/UAM when they are communicating with agents in their nearest neighborhood, a distributed consensus control is proposed that requires the transformed output measurements and dynamic controller states of the nearest neighboring agents to ensure reaching consensus while preserving the system's privacy.





Digital Twin Platform for Cybersecurity of Critical Infrastructure

Moein Manbachi, Ph.D., P.Eng., SMIEEE, Director
Minoo Shariat-Zadeh, P.Eng, SMIEEE, Project Lead
BCIT Smart Microgrid Applied Research Team (SMART)
minoo_shariat@bcit.ca



Project Description

Our project investigates safe way to test cyberattacks on critical infrastructure without risking real systems

- Problem:** Cyberattacks on critical infrastructure (e.g., power grids and other critical infrastructure systems) are increasing, and testing defences on real systems can cause disruptions and safety risks
- Solution:** This project develops a Digital Twin Platform to safely simulate cyberattacks in a virtual environment without impacting real operations
- Goals:** Identify system vulnerabilities, test defence strategies, and improve cybersecurity readiness for critical infrastructure
- Team & Context:** Led by BCIT SMART with academic and industry partners, funded under NCC/CSIN 2025 (Critical Infrastructure Protection)

Current Progress

- Needs Assessment:** Engaged with industry stakeholders to identify key cybersecurity challenges and priorities in critical infrastructure
- Gap Analysis:** Compared current systems to industry standards to identify major vulnerabilities and improvement areas
- Digital Twin Development:** Began building digital models of representative smart grid systems using data collected at BCIT
- Simulation Environment:** Developed a real-time testing platform to simulate cyberattacks and evaluate system responses safely

Implementation Plan

Phase	Focus
Phase 1(Descriptive, 2026–2027)	Build monitoring and situational awareness capabilities
Phase 2 (Predictive,2027–2028)	Develop predictive models and cyberattack simulations
Phase 3 (Comprehensive, 2028–2029)	Integrate AI-driven tools and immersive training environment

Budget

NCC Grant: \$900K | BCIT and Partner Contributions: \$910K | **Total Project Cost: \$1.81M**

Method

- Approach:** Co-developed with utilities, industry, and academic partners at BCIT's Digital Twin Innovation Hub (DTI-Hub)
- Execution:** Iterative, phase-based development with testing, partner feedback, and continuous improvement
- Testing:** Real-time simulation environment used to evaluate cyber threats and system responses safely
- Inclusion:** Emphasis on accessible training and participation from diverse communities

Future Exploration

- Predictive Capabilities:** Integrate real-time data to model and anticipate cyberattack impacts
- Advanced Platform:** Expand the digital twin with AI tools and interactive training features
- National Collaboration:** Develop a network of partners to share knowledge and strengthen cybersecurity across Canada
- Growth & Impact:** Support future research, industry partnerships, and potential commercialization opportunities

These steps will enable broader adoption and long-term impact across critical infrastructure sectors.

Project Collaborators

Lead Institution

- British Columbia Institute of Technology

Academic Partner

- Thompson Rivers University (TRU)

Industry Partners

- Awesense
- BC Hydro
- EdgeTune Power
- EVECTRIX
- Fuse Power Management
- Hydron Energy
- Powerinex AI
- Siemens Canada

Project's Cybersecurity Risk Assessment Benefits



Safe Testing

No risk to production systems or processes



Realistic & Representative

High-fidelity models and real traffic/behavior



Repeatable & Consistent

Reproduce scenarios and measure over time



Comprehensive Visibility

End-to-end visibility across IT, OT, and field devices



Faster, Better Decisions

Compare controls and prioritize investments



Compliance & Audit Evidence

Support standards and regulatory requirements



Cost & Downtime Reduction

Find issues early, avoid incidents and outages



Acknowledgements

This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN). Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RCC).

Additional support provided by BCIT DTI-Hub and collaborating partners, including BC Hydro, Siemens Canada, and others.



Zero-Knowledge Threat Detection and Risk Assessment in Aerospace and Orbital Infrastructures

Steven H. H. Ding (McGill University), Co-Investigators: Brian Lachine (RMC), Mohammad Zulkernine (Queen's University), Dakotah Soucy (RMC), Mark Adams (RMC)
Email: steven.h.ding@mcgill.ca



Project Description

Aerospace and orbital infrastructures are increasingly targeted by sophisticated cyber threats while relying on mission-critical systems and specialized communication protocols that are difficult to update. This project develops an AI-powered intrusion detection and risk assessment framework capable of autonomously learning previously unseen protocols, detecting cyber threats, and generating explainable security insights.

- **Project Focus:** Develop a zero-knowledge cybersecurity framework that can infer unknown aerospace and orbital communication protocols directly from raw data and generate adaptive intrusion detection capabilities.
- **Goals & Milestones:** Integrate protocol inference, self-reasoning threat detection, explainable AI, and human-AI collaboration into a unified system capable of operating across diverse aerospace platforms.
- **Technology Readiness:** Advance the technology from TRL 2 to TRL 6 over the three-year project.
- **Team & Context:** Led by McGill University in collaboration with the Royal Military College of Canada and Queen's University, with industry support from CAE, a leading Canadian aerospace technology company specializing in advanced aeronautical training and mission solutions, contributing expertise in mission-critical systems, aerospace operations, and cyber technology integration.

Current Progress

Year 1 Achievements

- Defined system architecture for protocol inference and AI-driven IDS.
- Developed initial machine learning models for protocol reconstruction.
- Established aerospace and orbital cybersecurity datasets.
- Conducted benchmarking and validation studies.

Budget & Method

- **Budget:** NCC Funding \$500K | CAE In-Kind Contribution \$47.8K
- **Protocol Inference:** Develop AI-driven methods to autonomously learn and reconstruct previously unseen aerospace and orbital communication protocols.
- **Self-Reasoning Threat Detection:** Integrate anomaly detection, threat reasoning, and explainable AI to generate adaptive intrusion detection capabilities and human-readable threat assessments.
- **Human-AI Collaboration:** Incorporate operator feedback to improve detection accuracy, interpretability, and system adaptability across diverse platforms.
- **Validation & Demonstration:** Conduct progressive testing using aerospace and orbital datasets.



Acknowledgements

This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSPR). Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RCC).

Add any other acknowledgements as appropriate.

Project Collaborators

Industry Partner
CAE Inc.

McGill University
Steven H. Ding (Project Lead)

Royal Military College of Canada
Brian Lachine
Dakotah Soucy
Mark Adams

Queen's University
Mohammad Zulkernine



Future Exploration

- **Operational Validation:** Expand testing beyond simulated environments using representative aerospace, satellite, and mission-critical communication systems to evaluate real-world performance and resilience.
- **Industry & Government Collaboration:** Strengthen partnerships with aerospace, defence, and critical infrastructure stakeholders to access operational datasets, domain expertise, and deployment opportunities.
- **Technology Expansion:** Extend the framework beyond intrusion detection to support risk assessment, threat intelligence, and cybersecurity monitoring across diverse cyber-physical systems.
- **Commercialization & Impact:** Advance technology transfer, intellectual property development, and commercialization pathways to support the adoption of adaptive cybersecurity solutions for aerospace and other critical infrastructures.



Protecting Alberta HigherEd with Global Partnerships

Kevin Paul, Director of Cybersecurity Operations, Cybera, kevin.paul@cybera.ca

Greg Lamb
SOC Manager, Cybera
greg.lamb@cybera.ca

Charlotte Beauparlant
SOC Delivery Manager, Cybera
charlotte.beauparlant@cybera.ca

Project Description

Cybera is working with Australia's National Research and Education Network, AARNET, to build a regional Security Operations Centre (rSOC) that will support higher education institutions in Alberta and Nunavut. The rSOC — which has the full support of all 26 post-secondary institutions in Alberta — will address the growing financial and operational difficulties faced by this sector in protecting their staff, student, and research data, in a uniquely strategic way.

Features of the rSOC

- Innovative operational model: Canada/Australia teams are able to trade off day/night duties, providing 24/7 detection and response to sector-wide threats, while ensuring Canadian data is 100% hosted in Canada
- Partnering institutions can contribute directly to the common detection and code base, further benefitting threat awareness for all members, and enabling hunt/response before a threat hits
- Cost savings: participating institutions will collaborate on a centralized solution, rather than repeating the same SOC model at an individual level
- Supports cybersecurity demand and skills development in all partner institutions, including those in northern Canada

Key milestones & deliverables

- Core SOC capabilities, with all data housed in Canada
- SOAR and UEBA functionality integrated
- A robust, sector-targeted use-case library, built in collaboration with security experts across the post-secondaries
- Collaborative roadmapping between Canadian and Australian research & education networks

Current Progress

- SOC architecture has been documented, and SIEM, SOAR & UEBA have been integrated, tested and are fully operational
- Established standardized procedures for handling alerts, conducting investigations, managing incident responses, and escalation
- Defined service performance metrics and created a dashboard and monthly report for onboarded members
- Three pilot participants in Alberta have successfully been onboarded

Budget & Method

- Estimated total project budget: \$7,702,054.00
- Total Amount from the NCC: \$2,500,000.00
- Total amount from Cybera: \$3,755,094.00
- Total amount from partners: \$1,446,960.00

Future Exploration

- Continuing to onboard new post-secondary institutions into the SOC as quickly as possible
- Duplicating AARNET's technology stack provided a quick start but introduced technology debt and risks. As the SOC matures, we are exploring new technology platforms to ensure program stability and scalability, guaranteeing all post-secondary members benefit from modern, robust security measures
- Cybera is open to partnering with additional Canadian and global National Research and Education (NREN) organizations to grow the SOC and expand the sector saturation. We believe more partners will enhance intel coverage and also make the 24/7 monitoring more equitable and sustainable



Acknowledgements

This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSN).
Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (NSC).

Cybersecurity Technology





CPI

Next Generation User Fingerprinting for Fraud Detection and Prediction

Diogo Barradas & Urs Hengartner (University of Waterloo)
Saqib Hakak & Roozbeh Razavi-Far (University of New Brunswick)



CIC

Project Description

Behavioural fingerprints represent people's unique behaviour while interacting with online platforms

- Key stroke, mouse input, or swipe dynamics
- Patterns of user actions

Behavioural fingerprints can be used for **malicious** and **benign** purposes

- User identification and authentication
- User tracking and profiling
- User impersonation
- Fraud detection

Research Goals

- Gather behavioural datasets from real-world websites, metaverse, and decentralized finance platforms
- Establish potential of using behavioural fingerprints for different purposes

Research undertaken by a team of researchers from the **Cybersecurity and Privacy Institute (CPI)** @ the University of Waterloo and the **Canadian Institute for Cybersecurity (CIC)** @ the University of New Brunswick in collaboration with **Mastercard**

Project Collaborators

- Yoonjib Kim, Krishno Dey, Refat Hemel (UNB)
- Alexandru Bara, Alim Dhanani, Neel Faganiya, Paul Wooseok Lee, Uzma Maroof, Hesam Sarkhosh, Surjot Singh, Aswad Tariq, Artemiy Vishnyakov (Waterloo)
- Michael Cacho (Mastercard)

Budget & Method

Budget

- NCC contribution: \$288,099
- Cash match: \$324,877

Milestones

- Simulation and data collection
- User authentication and profiling
- User impersonation
- Fraud detection and prediction
- Final report

Current Progress

- Crawled thousands of websites and analyzed them for the presence of behavioural biometrics scripts based on dynamic and static taint analysis.
- De-obfuscated obfuscated behavioural biometrics scripts to get an understanding of their functionality.
- Completed research on credit card fraud detection using graph neural networks (GNNs) by transforming tabular transaction data into graph representations that effectively capture relational patterns among instances.
- Completed a comprehensive survey on state-of-the-art user impersonation attacks in the metaverse.
- Developed a Minecraft-based simulation to collect behavioral data, helping analyze impersonation patterns and evaluate its usefulness in developing effective detection methods.
- Compared classifiers on crypto datasets and flagged NFT laundering in Decentraland using heuristics (price jumps, low liquidity, rapid sales, self trades) to detect suspicious patterns.
- Developed a simulation framework capable of generating complex, multimodal activity logs.
- Published papers in international venues (eCrime 2025, MadWEB 2026, SACMAT 2026)

Future Exploration

Next Steps

- Analyze collected datasets in terms of user profiling and fraud detection
- Build machine-learning classifier for real-time user identification in metaverse
- Build machine-learning classifiers for fraud detection and prediction
- Study threat of user impersonation based on behavioural data
- Release open-source software tools and collected datasets
- Describe research findings in conference and workshop publications

Project Needs

- Real-world datasets representing user behaviour on the web, in the metaverse, or elsewhere
- Real-world datasets representing fraud patterns

Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).

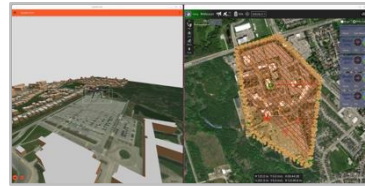
GPS Spoofing Detection Using Online Federated TinyML for UAV Swarms

Khail El-Khatib, Ontario Tech University, Faculty of Business & IT
khail.el-khatib@ontariotechu.ca

Project Description

Drones increasingly fly in coordinated swarms for public-service missions such as search-and-rescue, drone-as-first-responder response, and infrastructure inspection.

- The threat:** GPS spoofing lets an attacker hijack a drone's position sensor using cheap, off-the-shelf radio gear, putting an entire swarm at risk.
- The gap:** onboard drone computers have very limited power, compute, and network connectivity, which most existing defenses ignore.
- The goal:** an onboard intrusion detection system (IDS) that is accurate, efficient, and fast enough to flag spoofing in real time.
- The approach:** combine a compact TinyML model, on-device Online Learning, and privacy-preserving Federated Learning across the swarm.



A4-drone swarm mission in Gazebo + QGroundControl over the Ontario Tech University campus.



GPS spoofing moves the drone's reported position further outside its assigned mission area.

Current Progress

A working prototype runs end-to-end in simulation:

- Detection model engineered from GPS + IMU telemetry; pre-trained offline and quantized to TensorFlow Lite for low-power devices.
- An on-device Online Learning layer adapts to each drone in real time, while Federated Learning shares only model weights across the swarm.
- Validated in Gazebo + PX4 simulation with a mobile GPS spoofer and scaling to a 100-drone swarm.
- Preliminary accuracy (in simulation):** ~11% with TinyML alone, ~95% once Online Learning is added; the FL system holds ~95% while adding swarm-wide collaboration. Inference runs in under 1 ms on Raspberry Pi-class hardware.

Budget & Method

Method

- Threat model:** spoofing is simulated by pushing the drone's reported position outside its mission area. Rights are simulated in Gazebo.
- Model chosen by Neural Architecture Search (NSGA-III) over 100 trials, balancing F1 score, RAM size, and latency.
- Telemetry monitored over standard MAVLink and results logged for analysis.

Budget

- NCC contribution: \$89,987.50
- Matching contribution: \$

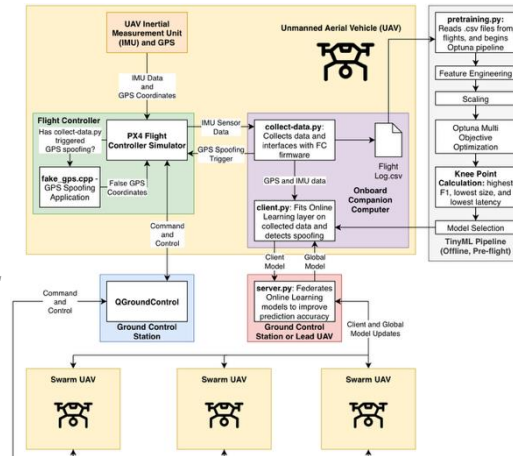


Acknowledgements

This project is supported by the support of the National Cybersecurity Consortium and the Government of Canada (CSIN).
Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).

Project Collaborators

- Dr. M. K. ... State University
- Dr. Abdulaziz Almeahmadi, University of Tabuk
- Durham Region Police Service



System architecture offline TinyML pipeline, on-device online learning, and a federated server.

Future Exploration

Planned next steps:

- Benchmark four standard metrics using simulation data and the public MAVIDS real-spoofing dataset: accuracy, F1, latency, and resource/energy use.
- Inject realistic GPS noise (e.g. cloud cover, weak signal) to test the system under non-ideal conditions.
- Harden federation security: secure aggregation, client authentication, and weighting to resist poisoned model updates.
- Real-time mission integration: automatic swarm-wide geofencing on confirmed spoofing, plus an operator dashboard to visualise attacks and configure the IDS.



Transfer Fuzzing for Devices Without Firmware

Meng Xu | Mei Nagappan · University of Waterloo
meng.xu.cs@uwaterloo.ca | mei.nagappan@uwaterloo.ca

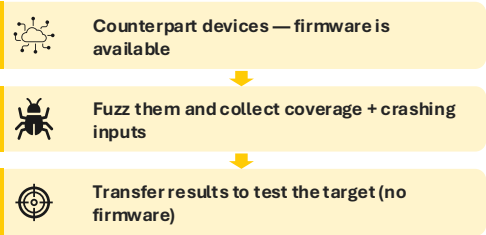
NCC Project 2023-1488

R&D
Critical Infrastructure
Protection
Started Aug 2024

Project Description

Many IoT devices cannot be security-tested because their firmware is impossible to obtain — a common problem for outdated and proprietary hardware.

- **Focus:** transfer fuzzing, a new way to find vulnerabilities in a device without access to its own firmware.
- **Key idea:** a device behaves like its counterparts, so we fuzz firmware from similar devices and transfer the results to test the target.
- **Goal:** enable thorough, automated vulnerability discovery across critical infrastructure, industry, and smart homes.
- **Context:** a Spearhead R&D project at the University of Waterloo within Canada's NCC program.



Project Collaborators

- **Project Lead:** Meng Xu, Mei Nagappan — University of Waterloo, Cheriton School of Computer Science.
- **Funding partner:** National Cybersecurity Consortium (NCC) & Government of Canada.

Budget & Method

- **Total budget:** CAD \$330,470.
- **NCC contribution** CAD \$270,470 + **matching** CAD \$60,000.
- **Method:** fuzz firmware collected from counterpart devices, then transfer coverage and inputs to test the firmware-less target.
- **Validated** on real Arm Cortex-M MCUs (STM32, NXP, Microchip).

Funding split — total CAD \$330,470

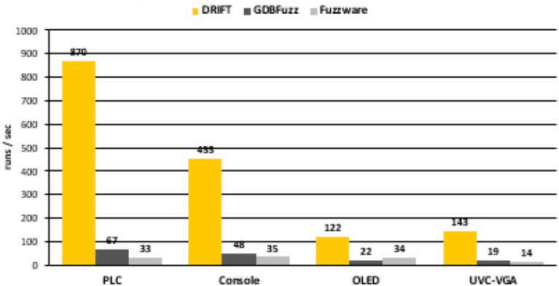


Current Progress

First outcome: DRIFT, a debug-based, on-device binary firmware fuzzer.

- **Uses the Arm Cortex-M** Debug Monitor so firmware traces itself — minimal overhead, high fidelity, high speed.
- **Found 3 unknown bugs** (all developer-confirmed) that other binary fuzzers missed.

Fuzzing speed (runs/sec) — DRIFT vs. binary fuzzers
Higher is better. Source-based SHIFT is faster but requires source code.



Future Exploration

The transfer-fuzzing vision extends well beyond a single device:

- **Auto-match** a firmware-less target to its best counterpart firmware using device fingerprints.
- **Transfer bug signatures**, not just inputs, across whole device families.
- **Generalize** transfer fuzzing to other black-box systems beyond IoT firmware.

Research Roadmap



Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).

We also thank collaborators at Northeastern University and the vendors who confirmed the reported bugs.



Project Description

- Improving Identity Access Management (IAM) in distributed systems is driven by the growing need to satisfy key organizational requirements (authentication, authorization, interoperability, privacy, availability, ... etc.). Traditional IAM models (centralized and federated) are often limited in terms of user control, data ownership, and cross-system trust, which becomes increasingly problematic in modern distributed and cloud environments. Self-Sovereign Identity (SSI) model emerges as a particularly important paradigm in this context. It refers a decentralized identity model where users fully control their digital identities. It involves an Issuer (issues credentials), a Holder (stores and uses credentials), and a Verifier (validates credentials).
- As distributed environments become increasingly dynamic and heterogeneous, IAM systems must be designed with greater structure, precision, adaptability, and security. This calls for a formal and automated generation of IAM architectures capable of satisfying a defined set of functional and security requirements.
- The project focuses on IAM systems more precisely SSI model. It proposes a Product Family Algebra (PFA)-based framework that formalize IAM requirements using feature models. Requirements are refined into security mechanisms, producing a feature tree that enables verification of IAM architectures. PFA constraints guide the process, ensuring verified requirements and validated constraints. The project reveals a process for SSI architecture generation defined from functional and non-functional requirements. Using catalogs of SSI and security patterns, architectures are automatically generated through pattern selection, integration and refinement.
- The project is carried out by researchers and students working in cybersecurity and identity management.

Project Collaborators

The project team consists of Kamel Adi, Nancy Badran, Maya Benabdelhafid, Pierre Saha Fobougou, Mohamed Mejri listed in alphabetical order.

Budget & Method

The project is conducted through a structured methodology combining applied research, technical development, and validation activities. The work is organized into clearly defined phases. These phases include requirements analysis, design and implementation, testing and evaluation, and reporting of outcomes. Regular coordination meetings are held to monitor progress and review deliverables. These meetings help ensure that the project remains aligned with its objectives and expected impact.

The project budget includes an NCC contribution of CAD 30,000 per year for three years. The budget is used primarily to support highly qualified personnel. This includes salaries for a PhD student and a postdoctoral researcher. Their work is central to the execution of the project. These salaries support research activities, technical development, experimentation, validation, documentation, and dissemination of results.

Current Progress

- Formalized IAM functional and security requirements using PFA as a structured feature tree, enabling the systematic refinement of high-level goals into concrete security mechanisms. For example, authentication requirement is supported through multiple mechanisms such as passwords, biometrics, multi-factor authentication, digital certificates, and decentralized identity approaches like Verifiable Credentials (VC) and Decentralized Identifiers (DID) in the case of SSI model.
- Focused on the SSI model and established an automated architecture generation process that transforms functional and security requirements into architectural building blocks. The approach leverages catalogs of SSI and security patterns to support automated pattern selection and integration according to the identified requirements.
- Constructed a Knowledge Graph (KG) that captures SSI domain knowledge and relationships. The graph links among others SSI actors (Holder, Issuer, and Verifier), exchanged objects (DIDs, VCs, cryptographic keys), components (e.g., wallet) and patterns (e.g., key management, DID document management, credential design). This semantic layer improves traceability between stakeholder requirements, security decisions, and architectural elements.

- Defined a multi-stage architecture refinement process in which selected patterns are first assembled into an abstract SSI architecture and subsequently transformed into a complete software architecture. The generated architectures incorporate the core SSI entities together with the required security services needed to satisfy the specified requirements.

Future Exploration

- The next step is to refine the code generation prototype that demonstrates the full automated generation of SSI-based IAM architectures from requirements, validating the end-to-end process from high-level organizational requirements to concrete SSI components.
- To further strengthen this process, the KG will be enriched with additional SSI concepts. For example, the lifecycle of a VC including states (requested, issued, stored, presented, lost, and revoked) can be added to improve semantic reasoning, traceability, and decision support during architecture integration. We will also implement dedicated APIs for the SSI and security patterns to enable the architecture refinement.
- Finally, we will evaluate the resulting prototype under realistic deployment scenarios and ensure its applicability in real-world distributed systems.

Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN).

PASCAL Project: Defending Canada's Critical Infrastructure with Physics-Based Supply Chain Cybersecurity

Matthew Monteyne (PL), Palitronica, matthew.monteyne@palitronica.com

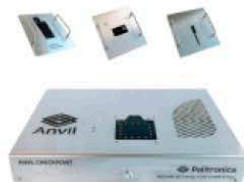
Learn more: palitronica.com

Contact: info@palitronica.com

Visit us: 140 Columbia St. W
#301B, Waterloo, ON

Project Description

- Palitronica and the University of Waterloo are commercializing **Anvil CheckPoint**, a hardware integrity verification system for electronics in critical systems.
- Develop a turnkey solution to detect counterfeit, recycled, or tampered electronic components in critical-systems supply chains.
- Address urgent needs in aerospace, defense, automotive, and high-security industries facing global chip shortages and grey market threats.
- The project is structured to progress from low-volume evaluations to full operational deployment, culminating in the assessment of up to 10,000 parts across pilot and production environments.



Project Collaborators

Palitronica Inc. (Waterloo, ON)
University of Waterloo – Real-time Embedded Systems Lab
Continental

Budget & Method

- Total Project Value:** \$1.7M
- Funding Breakdown:**
 - Palitronica: \$2.57 Million
 - NCC: \$1 Million
 - Velocity: \$150K
- Execution Strategy:**
- In collaboration with Continental, two distinct devices under test (DUTs) are being evaluated:
 - One focused on an automotive safety application
 - One focus on an automotive security application.
- DUTs are tampered and evaluated in blind test
- Anvil CheckPoint is tailored to end-user need and improved through repeated testing

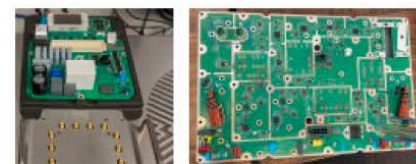
Current Progress

- TRL 8 achieved
- On schedule with 40% of project completed
- Long Term Partners (LTP) are all established with goals and objectives defined
- Currently evaluating 7 different DUT's across 4 LTP



Future Exploration

- Full integration of the **Anvil CheckPoint** in standard testing across manufacturing locations with Continental
- Further integration into multiple lines of business with Rolls-Royce
- Exploration study for validating COTS assemblies
- Fully automated integrations



Acknowledgements

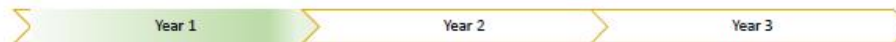


This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RSC).



Fully Automated End-to-End Vulnerability Discovery and Repair with LLMs

Steven Y. Ko, Associate Professor, steveyko@sfu.ca



Benchmark Design & Automated Vulnerability Detection

Automated Vulnerability Repair & Validation

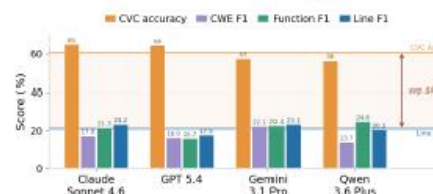
End-to-end Framework

Project Description- RustMizan

A compilable, contamination-aware benchmarking framework for Rust vulnerabilities.



- Targets Rust memory-safety CVEs in security-critical infrastructure
- 42 real-world CVEs packaged as 173 compilable variants at three context levels: crate, file, function.
- Four tasks per vulnerability: detection, CWE classification, function and line-level localization.
- Paired mutation framework generates semantics-preserving variants for contamination + adversarial-robustness testing.



Current Progress - SysEduBench

Evaluating LLMs on building computing systems

- Two paired sub-benchmarks: SysExam and SysLab.
- Four core systems domains: intro to systems, operating systems, distributed systems, databases.
- Reveals a knowledge-vs-implementation gap: models score 2–22 pp lower on labs than on exams.
- Open platform: instructors contribute their own exams and labs; leaderboard shows full agent trajectories.



Future Exploration

- Expand Mizan: broader vulnerability classes and a larger curated CVE dataset.
- Grow the mutation framework: new benign / malignant / Rust-specific mutations to keep the benchmark contamination-resistant as models retrain.
- Explore LLM-driven vulnerability repair: agentic patch generation validated against Mizan

Project Collaborators

- Tarek Elsayed, SFU
- Shiping Yang, SFU
- Mohammad Omidvar, SFU
- Zeyu Chen, Trinity University
- Angélica Moreira, Microsoft Research
- Xuan Feng, Microsoft Research
- Angel Chang, SFU
- Nick Sumner, SFU
- Steven Y. Ko, SFU

Budget & Method

NCC Spearhead funds \$500,000

Costs so far	
Wages	\$110K
LLM Resources	\$8K
Travel	\$1.8K
Indirect Costs	\$7K



Acknowledgements

This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSPN). Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RCC).



Enhancing Electric Vehicle Charging Infrastructure Cybersecurity Through Autonomous and Sustainable AI

Li Yang, Ontario Tech University, li.yang@ontariotechu.ca

GitHub Accounts:

LiYangHart

ANTS-OntarioTechU

Project Description

Project Focus:

- Strengthening Electric Vehicle Charging Station (EVCS) cybersecurity using AI-driven, energy-efficient, and privacy-preserving Intrusion Detection Systems (IDSs).

High-Level Goals and Milestones:

- Analyze EVCS cyber vulnerabilities and threats
- Develop and test cybersecurity methods using advanced Machine Learning (ML) models, including Automated ML (AutoML), TinyML, Federated Learning (FL), and Multi-Objective Optimization (MOO)
- Validate in real-world EVCS environments

Context:

- Aligns with Canada's EV adoption goals
- Supports sustainable, resilient, and secure EV infrastructure

Project Collaborators

- Project Lead: Li Yang, Ontario Tech University
- Co-Lead: Khalil El-Khatib, Ontario Tech University
- Investigator: Katarina Grolinger, Western University
- Collaborator: Automotive Centre of Excellence (ACE)

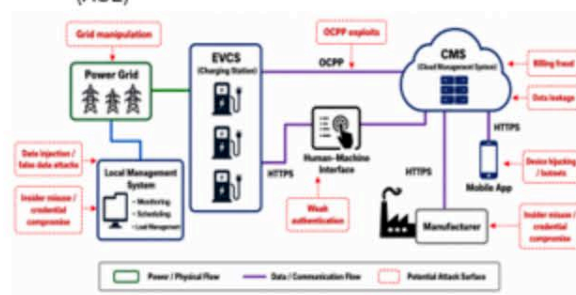


Fig.1. EV Charging System Cybersecurity Vulnerabilities

Budget & Method

Budget Overview:

- NCC Contribution: CAD \$175,294.10
- ACE matching contribution: CAD \$30,000

Development Phases:

- Design IDS prototypes using AutoML, TinyML, and FL
- AutoML: automatically optimizing AI/ML models
- TinyML: develop lightweight ML on edge devices
- FL: privacy-preserving decentralized learning
- MOO: balance model performance and efficiency

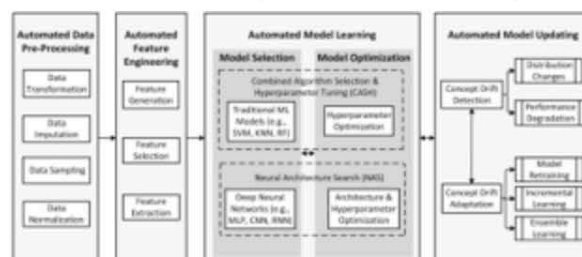


Fig.2. Overview of the AutoML framework

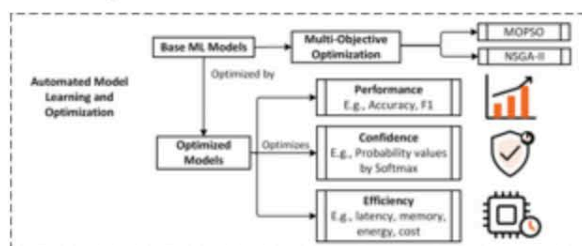


Fig.3. MOO framework for effective and efficient ML

Evaluation Metrics:

- Detection accuracy, latency, energy consumption, privacy impact

Training HQP:

- Support 3 MSc and 2 PhD student
- Offer hands-on experience in AI and cybersecurity

Current Progress

- Conducted a comprehensive literature review on current EVCS security challenges and solutions;
- Analyzed current cybersecurity measures in EVCS;
- Developed multiple IDS solutions to address common cyber-attacks in EVCS using novel AI/ML methods, including AutoML and TinyML techniques.
- Completed two survey papers and two research papers
 - A Comprehensive Survey on Online AutoML and Adversarial Robustness for IoT and EV Charging Network Security (Published)*
 - EGGA: An Error-Guided Generative Augmentation and Optimized ML-Based IDS for EV Charging Network Security (Published)*
 - A Multi-Objective AutoML-based Efficient Intrusion Detection System for EV Charging Networks (accepted in GlobeCom 2026)*
 - TinyML for Cybersecurity in EV Charging Networks (under review)*

Future Exploration

Below are the next steps of this project:

- Develop specific IDS prototypes for EVCS systems;
- Test IDS prototypes under various simulated attack scenarios;
- Refine and optimize IDS prototypes for improved effectiveness and efficiency;
- Finalize the deployment strategy for optimized IDS prototypes in testable EVCS systems;
- Develop partnerships and collaboration frameworks with EVCS operators for real-world testing.

Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSN). // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RSC).

Fortifying Cybersecurity: Early Ransomware Detection and Mitigation Methods

Saqib Hakak, Faculty of Computer Science, Canadian Institute for Cybersecurity, University of New Brunswick,
saqib.hakak@unb.ca



Project Description

Project Focus

- Early detection of ransomware before encryption begins
- Uses **MITRE ATT&CK framework** to analyze ransomware attacks
- Combines static and dynamic behavioral analysis
- Aims to reduce data loss and enable real-time defense

Goals & Milestones

- Investigate which MITRE ATT&CK sub-techniques are most commonly used in ransomware attacks
- Determine which sub-techniques are most applicable or effective in executing ransomware
- Analyze attacker behavior to understand the tactics, techniques, and procedures (TTPs) used in real-world ransomware incidents
- Focus on sub-techniques used during initial access, execution, persistence, and encryption phases and create a new Ransomware Dataset
- Develop detection model based on attacker behavior patterns as per **MITRE ATT&CK framework**
- Evaluate effectiveness in simulated and live environments
- Industry testing and validation in final project year

Project Team

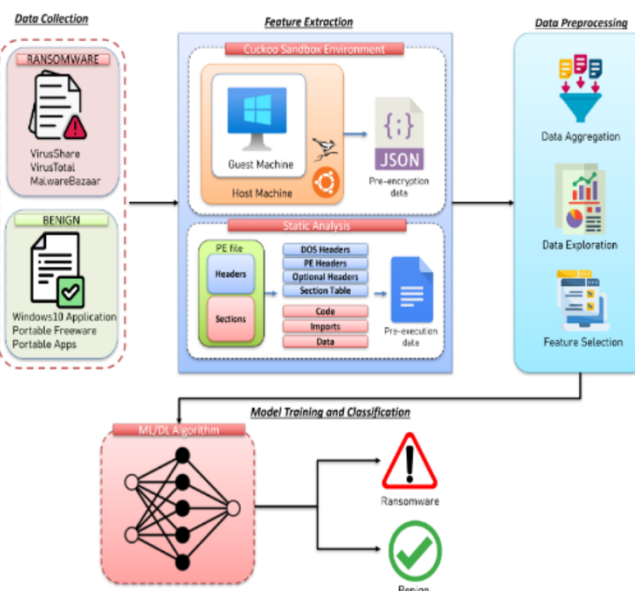
- Saqib Hakak (Associate Professor), University of New Brunswick
- Graduate Student: Sk Mahtab Uddin

Project Collaborators

- Dr. Miguel Garzón
School of Electrical Engineering and Computer Science
University of Ottawa
- Industry Partner: EzSec Inc.

Budget & Method

- Total Project Cost = \$221,400
- NCC contribution = \$79,500
- Matching Contribution = 141,900



Current Progress

- A comprehensive literature review on early ransomware detection techniques has been completed.
- As part of dataset development, 11,191 ransomware samples have been collected from reputable sources including VirusShare and MalwareBazaar to date.

- A controlled sandbox environment has been created consisting of Ubuntu 20.04 host machine with a Windows 10 guest virtual machine for conducting dynamic behavioral analysis.

Future Exploration

- We aim to develop a custom ransomware dataset specifically focused on pre-encryption behavior, guided by the MITRE ATT&CK framework
- We will investigate highly relevant features and the selection methods to enhance early ransomware detection accuracy and reduce false positives.
- We also plan to explore zero-shot learning techniques to improve generalization, allowing detection of novel ransomware families without retraining
- Analyze additional MITRE ATT&CK techniques to identify other patterns and behaviors useful for early-stage ransomware detection.
- Plan to hire additional HQP (graduate students, researchers) to support dataset creation, model development, and evaluation.

Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).



Part of this project is also supported by New Brunswick Innovation Fund (NBIF) under grant number RAI_2023_059

Threat Modelling and Mitigation of human-factors based exploits in advanced driver assistance systems

Project Lead: Atrisha Sarkar · Assistant Professor, Electrical & Computer Engineering, Western University · atrisha.sarkar@uwo.ca

Co-PIs: Mohamed Zaki · Associate Professor, Civil & Environmental Engineering | Apurva Narayan · Associate Professor, Electrical & Computer Engineering, Western University

01 Project Description

- Across North America, more than a third of vehicles run Level-2 ADAS — systems that still rely on the human driver as the final line of defense, opening a new class of cybersecurity vulnerability at the intersection of human behavior and vehicle autonomy.
- Attackers can monitor driver behavior — reaction time, driving style, skill, tendency to over-rely on automation — and tailor attacks to it. Sensor and perception exploits are well studied, but these behavioral attack vectors sit outside today's cybersecurity frameworks, leaving manufacturers unaware about mitigation of such type of attacks.
- This project closes that gap for Canada's automotive sector through scientific advances at the intersection of human factors and game-theoretic adversarial modeling. It applies these advances for practical threat assessments and protocol designs that help increase the safety and security of the widely deployed Level-2 ADAS.

02 Project Collaborators

PI and co-PIs:

- Atrisha Sarkar · Assistant Professor, Electrical & Computer Engineering, Western University
- Mohamed Zaki · Associate Professor, Civil & Environmental Engineering, Western University
- Apurva Narayan · Associate Professor, Electrical & Computer Engineering, Western University

Research Assistants:

- Nour ELGharably · Pranav Jha · Pratik Gupta · Mayar Nour

Participating organizations:

- Acerta

03 Budget & Method

NCC contribution	\$ 481,850CAD
Anticipated match	\$ 500,000CAD

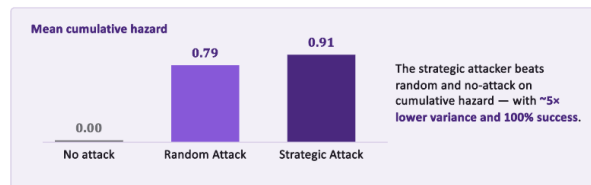
Project Outcomes

- Behavioral Game-Theoretic Attack Model** — Game theoretic attack model that generates optimal attack strategies based on driver behavior profiles inferred from control-input data (steering patterns, lane changes, braking behavior).
- Pre-emptive Take-Over Request (ToR) Protocol** — By conducting a HIL driving-simulator based study, driver reaction and response times will be measured in the context of security-triggered ToRs across varying cognitive load. This study will help examine the safety of current ToR protocols under security attacks, and will be used to develop a more resilient, security-aware, risk-based ToR protocol.
- Risk Assessment & Remediation Framework** — Evaluates leading cybersecurity threat analysis methods (TARA, SARA) for human factors related vulnerabilities against ISO/SAE 21434:2021. Then, a full threat assessment will be run on the formalized set of adversarial scenarios developed by the GT Attack Model, giving manufacturers actionable procedures and equip regulators with compliance tools.

04 Current Progress

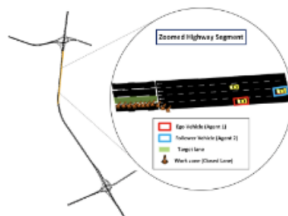
❖ Behavioral game-theoretic attack model

- A model that automatically generates optimal man-in-the-middle attack strategies from driver profiles to elicit an unsafe response.
- Posed as a Stackelberg game — attacker (leader) vs. the take-over logic (follower), with the driver as a stochastic player.
- The attacker reverse-computes the smallest perturbations needed to force a unsafe decision, kept within stealth bounds to evade detection.
- Receding-horizon planning with continuous Bayesian inference of the driver's type.
- Two attack pathways: suppress the system's response to real danger or force an emergency and corrupt the chosen maneuver.
- Consistently outperforms random and no-attack baselines in cumulative hazard, with far lower variance.



❖ Co-Simulation & Game-Theoretic experimental testbed

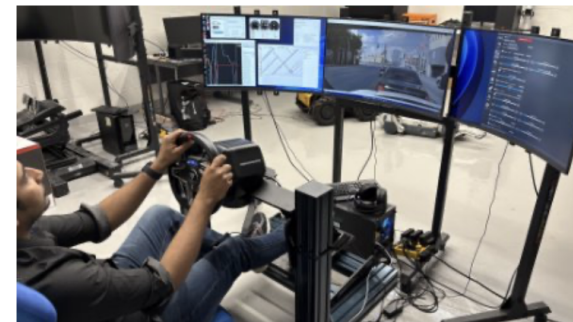
- Developed a microscopic traffic co-simulation prototype using the SUMO simulator and vehicle strategic planners, successfully calibrated against real-world, naturalistic trajectory data from an intersection in Waterloo, Ontario and 7 km M50 4-lane motorway in Dublin, Ireland
- Implemented a custom strategic vehicle behavioral planner using a Nash equilibrium-based solution concept to represent baseline rational behavior, while surrounding traffic is managed via out-of-the-box simulator models.
- Established a testbed repository featuring unplanned work zone scenarios, lane closures, and density variations designed to force complex interactions and vehicle takeover requests.



05 Future Exploration

➤ Next steps

- A tool for identifying and quantifying optimal behavioural exploits that can be used by attackers to compromise ADAS systems. Develop an Intrusion Detection System (IDS) to mitigate against such attacks.
- Run a driving-simulator study of driver reaction and response times under security-triggered ToRs, across varying cognitive load and situational complexity.
- A driver take-over protocol following the detection of a security breach, incorporating behavioral and situational variables.
- Evaluate ISO/SAE 21434:2021 standards against human-factors based vulnerabilities and attacks identified in the project



Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).



Project Description

Modern cryptography provides functionality far beyond traditional data privacy, including homomorphic encryption, zero-knowledge proofs, and verifiable delay functions.

- Applications: cloud computing, blockchain, anonymous verifiable voting, and more.

Many proposed solutions for these cryptosystems rely on *groups of unknown order*, mathematical structures whose size cannot be efficiently computed, e.g.

- ideal class group of an imaginary quadratic field,
- Jacobian of a genus 3 hyperelliptic curve.

Highly attractive, as these do not require enlisting a trusted third party to construct.

Unknown which groups are best-suited for applications, or if better alternatives exist.

Project Goals

- Obtain compelling evidence of security and efficiency of proposed cryptosystems relying on groups of unknown order.
- Determine best settings for applications via analysis and prototype implementation.
- Investigate novel settings that may have additional advantages including efficiency and quantum-resistance.

Current Progress

The project is currently in its preliminary stages, specifically literature review and exploring initial findings. Next steps include:

- Determine which of ideal class group or Jacobian of a genus 3 hyperelliptic curve is best suited for implementing verifiable delay functions.
- Investigate the security and efficiency of the infrastructure of a real quadratic field as a setting unknown-order protocols. May offer improved performance via better security properties.

Budget & Method

Total NCC Grant: \$499,411

Total Matching Contributions: \$271,500

Method

- Perform a rigorous analysis to ensure the security of the resulting protocols.
- Determine how to select appropriate parameters for optimal security and efficiency.
- Develop and test prototype implementations of the algorithms to assess their suitability for real-world applications.

The budget will be used to fund the researchers working on the project, including student and postdoc salaries and travel allowances to disseminate research.

Project Collaborators

Current Members:



• Michael John Jacobson Jr. - Professor, University of Calgary



• Laurent Imbert - CNRS researcher, University of Montpellier, France



• Renate Scheidler - Professor, University of Calgary



• Ha Tran - Assistant Professor, University of Alberta Augustana



• Brian Kehrigh - Masters Student, University of Calgary



• Srijan Khatri - Masters Student, University of Calgary

Future Members (Sept. 2026):



• Clare Dufresne - Masters Student, University of Calgary



• Eli Oryds - Postdoctoral Fellow, University of Calgary

Future Exploration

Future work will focus on integrating these cryptosystems into real-world systems and exploring commercial potential.

The project has the potential to generate novel intellectual property, industrial partnerships, and follow-up collaborations with academic researchers and cryptography practitioners.

Possible non-academic partners include organizations specializing in:

- Identity management systems
- Electronic commerce and asset transactions
- Blockchain deployment

We will actively seek new academic collaborators and commercial partners during the duration of the project in preparation for these next steps.



Acknowledgements

This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CGN).
 Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (CGC).

The image included within (not the people) was generated using generative AI.

Defence, Arctic and Sovereignty





Marine Cybersecurity



Jonathan Anderson, Memorial University of Newfoundland
jonathan.anderson@mun.ca



SCMS: Securing Critical Marine Systems NCC 2024-1326

Canada's is dependent on the maritime sector and exposed to vulnerabilities in marine control systems. This project will:

- develop **protocols** and **platforms** for trustworthy, resilient marine systems
- prototype electronic navigation and control systems with hardware and/or software compartmentalization (e.g., Capsicum, CHERI, CHERIoT)
- visualize cybersecurity state to seafarers
- demonstrate practical integration of secure systems on the water

Budget & Method

NCC	\$759,100
Memorial University	\$586,400
Dalhousie University	\$172,800
GovNL	\$138,806

- HQP support
- Marine equipment
- Research dissemination costs

SCMS Collaborators



Dalhousie University
Faculty of Computer Science



Current Progress

Control protocol (paper under submission)

Developing data-gathering "black box"

CSA TS-028: MASS Cyber



Stakeholder workshop inc. CCG, RCN

Future Exploration

Potential application for sensitive use cases with a new partner (platform vendor)

Potential expansion to protection of naval control protocol via DDS and Modular Open Systems Architecture (MOSA)

Potential collaboration with another Canadian university

MCT: Marine Cybersecurity Training NCC 2024-1354



Over 80% of international trade is carried by maritime transport, with over 100,000 vessels of 100 gross tons or more, crewed by over 1.9M seafarers around the world. Seafarers undergo extensive training, but not on cybersecurity. This project will develop three training modules:

1. Cybersecurity essentials for the marine industry (both seafarers and shore side)
2. Intensive, simulator-based emergency procedure training for seafarers
3. Corporate emergency procedure training and validation (table-top)

Budget & Method

NCC funding:	\$576,528
Memorial matching:	\$578,699

- HQP support
- Simulation and technology costs
- Research dissemination costs

Current Progress

Team recruitment and preparation for simulation work (collab. with NRC project)



Site visit by vessel operator interested in piloting our training courses

Future Exploration

Relationship to emerging global MASS code (Marine Autonomous Surface Ships)

Impact on global seafarer training standards

Potential expansion to naval use cases

MCT Collaborators



Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).

These project were also made possible by matching contributions from Memorial University and Dalhousie University.



Project Description

Addressing Cyber Threats to Democracy

The project examines the role, influence, and impact of human factors on the cybersecurity of democratic elections in Canada.

Cyber threats include threats to election infrastructure, voters, candidates, and parties; the creation of misinformation, disinformation, malinformation, and deepfakes and their spread through social media platforms.

Project Goals

-  Understand the role and influence of **human factors** on Canadian election cybersecurity
-  Improve election cybersecurity policies and propose law reforms related to cyber threats to democracy
-  Utilize knowledge of human factors to develop a **technological concept** to improve voter cognitive security and democratic deliberation

Current Progress

- Developed a prototype for the project's technological concept (serious computer game to increase cognitive security), conducted a survey of disinformation games as well as an intellectual property landscape
- Book proposal accepted by an academic publisher for a book collection on Foreign Interference in Canadian Democracy. Development of a book collection on **Securing Artificial Elections** is underway
- Conducted an inaugural workshop in September 2025. Planning underway for a workshop on securing artificial elections and on combatting adversarial epistemic attacks on the cognitive security of democratic electors
- Ongoing consultations with public and private sectors

Budget & Method

Methods

Research methods are rooted in the rule of law, and based upon robust, evidence-based, technologically-informed, transdisciplinary, and human-centered methods.

\$500,000
Total NCC Grant

\$120,000
Matching contribution



Acknowledgements

This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSNG).
Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RCC).

Project Collaborators

J.C Boucher, PhD: Data Science & Global Affairs

Holly Ann Garnett, PhD: Election Integrity

Rei Safavi-Naini, PhD: Information Security & Cryptography

Heidi Tworek, PhD: History, Human Factors & Technology

Stephanie Carvin, PhD: National Security

Allen Habib, PhD: Political Philosophy & Epistemology

Michael Pal, SJD: Election & Constitutional Law

Christopher Tenove, PhD: Platform Policies & Elections

Leah West, SJD: Cybersecurity Law & Cyber Operations

Future Exploration

- Continue **human-centric research** to answer project questions
- **Organize and host future workshops and meetings** for collaborative development of technological concept and scholarship
- Continue **engagement with policymakers and government** to support law reform, policy development, and research
- **Improve on the technological concept and prototype** to enhance cognitive security of electors
- **Engaging with industry** to discuss the potential commercialization of the technological concept
- Continue **producing scholarship** and submit for publication


CitizenOne
Bruce Levis | Chief Revenue Officer

bruce.levis@portagecybertech.com

PORTAGE
cybertech


PROJECT DESCRIPTION

CitizenOne is a government-grade Customer Identity and Access Management (CIAM) and digital services platform purpose-built for public-sector organizations. It provides a modular toolkit to identify, verify, onboard, and authenticate users while responsibly consolidating e-services in one secure access point.

The platform enhances:

- **Security:** Improves the cyber-resilience of organizations and ensures compliance in regulated environments.
- **Privacy:** Helps avoid the duplication of multiple stores of citizen identity data and enhances privacy by implementing a consent-driven approach.
- **Accessibility:** Delivers an inclusive user experience that protects vulnerable users from inappropriate use of identity data.

CitizenOne serves public sector organizations (federal, state/provincial, municipal), as well as higher education institutions and regulated industries.

Raising awareness to drive adoption of CitizenOne across North America requires navigating complex procurement and regulatory environments. High-level project goals include:

- **Content & awareness:** Develop videos, social media articles, and white papers.
- **Market research & engagement:** Conduct research across regions and generate impressions across target sectors.
- **Events & demos:** Participate in events and deliver product demonstrations.
- **Adoption pipeline:** Engage qualified accounts.

The U.S. market's diverse networks, procurement processes, and regulations create uncertainty and barriers to scale and underline the importance of targeted research, trusted partnerships, and localized engagement.

CURRENT PROGRESS

- **Technical content:** Market observations drove the launch of a new corporate website, sales deck, buyer's guide and various white papers.
- **Brand awareness:** Awareness is growing organically through iterative, multi-channel marketing initiatives.
- **Aggressive engagement strategy:** webinars and roadshows help move accounts into advanced sales stages.
- **U.S. market expansion:** Progress is advancing through partnerships and a stronger regional presence supported by two newly hired local sales representatives.

BUDGET & METHOD

1M\$ over 2 years to bolster our sales and marketing efforts

Enabling sales, marketing, procurement, and project partners to collaborate more effectively to drive market penetration and client engagement.

PROJECT PARTNERS

Pellera

with **Justin Hall**, VP of Strategic Partner Growth and his team.

UQO

Université du Québec en Outaouais (UQO) with student contributors.

Portage CyberTech

An internal team of over 15 people in Marketing, Sales, Delivery and Support:

- **Bruce Levis**, Chief Revenue Officer
- **Gregory J. Natran**, Lead Service Transformation Architect
- **Ed Therriault**, Business Transformation Architect
- **Jim Lawson**, Product Marketing Director, CitizenOne

ACKNOWLEDGEMENTS



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN)

Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).

FUTURE EXPLORATION

The next phase will focus on converting awareness and engagement into sustained market adoption.

Key priorities include:

- Scaling partner-led distribution and reseller channels.
- Expanding U.S. market presence through localization.
- Deepening engagement with priority public sector accounts.
- Advancing toward pilot deployments and broader adoption.

As the project progresses, we will continue refining its commercialization strategy based on customer feedback, procurement realities, and regional market requirements.

IntruderInsight

Elevating Cyber Attribution with AI Insights

Project Lead: Herbert Fensury | ENFOCOM Cyber
 Email: herbert.fensury@enfocom.com

For additional information go to www.enfocom.com
 Email: info@enfocom.com

Project Description

Timeline: Mar 31, 2025 – Mar 31, 2028

Environment:

- Attribution remains a major challenge in cyber threats.
- In 2024, 72% of Canadian companies experienced a cyber-attack.
- Identifying perpetrators is still difficult, limiting response timeliness and accountability.
- IntruderInsight offers advanced technology and collaboration to strengthen threat attribution and reduce future cyber risks.

Project Focus:

- Develop efficient cyber threat attribution methods to support government, law enforcement, and industry.
- Create a curated IoC dataset and a honeynet-based environment to drive innovation and strengthen cyber defence.

Goals & Milestones:

1. **Build** a multi-instance honeynet for IoC collection.
2. **Develop** a curated, multi-level IoC dataset for ML/DL training.
3. **Create ML/DL models** for cyber threat attribution.
4. **Apply models** to attribute unknown incidents and detect novel threats.

Team:

- Led by ENFOCOM Cyber with proven law enforcement cybersecurity training experience.

Project Collaborators

Law Enforcement Agencies:

- Calgary Police Service (CPS)
- Edmonton Police Service (EPS)
- Royal Canadian Mounted Police (RCMP)

Academic & Professional Training Institutions:

- University of Alberta
- Université du Québec en Outaouais
- University of Calgary - ENSF

Cybercrime & Cybersecurity Training Experts:

- Field Effect Software Inc.
- IBM Canada
- Intlabs
- Cybera

Budget & Method

Total Budget: \$6,954,876 CAD

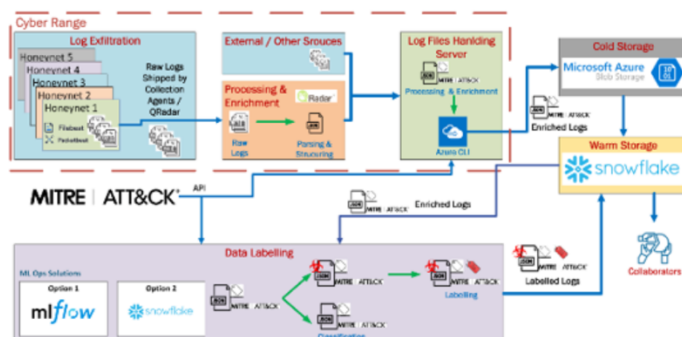
NCC Funding of \$2,000,000 CAD, allocated as:

- **Establish Honeynet Environment (10%)** - \$200,000
- **IoC Dataset Development (20%)** - \$400,000
- **ML and DL Analysis (30%)** - \$600,000
- **Evaluation and Generalization (20%)** - \$400,000
- **Operational Costs (20%)** - \$400,000

Methodology:

1. **Honeynet Deployment:** Deploy simulated environments to capture detailed IoC and TIP data.
2. **IoC Dataset Curation:** Curate collected data into multi-level IoC datasets (e.g., hashes, IPs, domains, tactics).
3. **ML/DL Analysis:** Apply advanced models to identify patterns and anomalies for accurate threat attribution.
4. **Model Evaluation:** Test models on unknown threats to assess real-world performance and attribution accuracy.

Current Progress



- Honeynet architecture design and deployment.
- Preliminary IoC data collection and analysis.
- Roundtable discussions with law enforcement officers and cybersecurity experts.

Key Learnings & Adjustments:

- **Faster Attribution:** Accelerate response and investigation times through automated and efficient IoC analysis.
- **Scalability:** Process large-scale datasets in real-time.

Future Exploration

Next Steps:

- Initial data collection.
- Data collection and sanitization pipeline for curated dataset creation.
- AI pipeline design and development

Gaps & Learnings:

- **Environment Detection:** Threat actors may detect virtualized or artificial data collection environments, leading to altered behavior and unreliable data.
- **Advanced Obfuscation:** Attackers use sophisticated techniques to conceal their identity, reducing the effectiveness of low-level IoCs like IPs and hashes.
- **False Attribution:** Skilled attackers can mimic others' tactics, misleading investigators and complicating attribution using high-level IoCs.
- **Cross-Sector Collaboration:** National partnerships bring together diverse expertise for IoC collection, AI training, and attribution.
- **Broader Impact:** Enhances security, reduces cyber-related costs, and supports economic growth through potential commercialization.

Expansion Opportunities:

- **Broaden Collaboration:** Partner with international organizations to access diverse expertise and resources.
- **Commercialization:** Offer developed technologies as products or services, generating revenue and positioning Canada as a global leader in cyber attribution.
- **Training Programs:** Launch workshops, webinars, and certifications to build capacity among cybersecurity professionals and law enforcement.
- **Integration with Cyber Initiatives:** Align project outcomes with existing cybersecurity frameworks to boost coordinated threat detection and response.
- **Enhanced Data Collection:** Expand datasets by integrating threat intel, network traffic, and OSINT to strengthen attribution accuracy.
- **New Use Cases:** Apply developed tech to areas like fraud detection, insider threats, and supply chain security.

Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).



Project Description

Project Focus

Commercialization of CYBERDEFENSE AI Platform, the first fully autonomous AI-Driven Preemptive Cybersecurity Platform, entirely engineered in Canada. Built to replace outdated signature-based technologies such as WAF, IPS, and IDS solutions, CYBERDEFENSE AI™ represents a fundamental paradigm shift in cybersecurity: preempting, adapting to, and neutralizing zero-day threats autonomously in real time, no signatures, no rules, no human intervention.

High-Level Goals & Milestones

- Launch international commercialization campaign; official European market entry confirmed at VivaTech 2025 (Paris).
- Expand market visibility through events in Canada and Germany like: The ALL-IN Bug Bounty at Hackfest 2026 is not an event. It is a declaration. Live, streamed, and scored, 50 of the world's best ethical hackers will attack CYBERDEFENSE AI™ for 12 hours. The results will be published. This is how CYBERDEFENSE AI establishes the new standard, while legacy technologies stay behind NDAs.

Current Progress

Blueteam GmbH has confirmed its first planned deployments in German hospitals and is actively developing a pipeline of CISO/CTO prospects across Germany — marking the beginning of CYBERPASS™'s operational expansion into Europe's Healthcare and critical infrastructure sectors.

CYBERDEFENSE AI CYBERPASS™ has been validated against real-world zero-day attack vectors and demonstrated superior performance over competing WAF, IPS, and IDS solutions in autonomy, response speed, and zero-day protection.

SIMNET has expanded its European private cloud infrastructure to support CYBERDEFENSE AI deployments, providing sovereign hosting capabilities across Germany and the continent.

Budget & Method

The project is supported by a total budget of CAD \$475,000, including \$142,250 requested from the National Cybersecurity Consortium (NCC), representing 30% of total project costs, and \$332,750 in matching contributions from CYBERDEFENSE AI and ecosystem partners SIMNET, BlueTeam GmbH, and CYBERECO. NCC funding will support German commercialization activities including marketing campaigns, third-party validation, certifications, sales enablement, onboarding activities, and infrastructure readiness.

Future Exploration

CYBERDEFENSE AI is entering a new phase of international expansion, including a potential defense and military cybersecurity partnership organization. Beyond commercialization, our ambition is to help build a globally recognized Canadian cybersecurity industry capable of securing digital infrastructure worldwide.

CYBERDEFENSE AI's goal is to help Canada emerge as a global leader in AI-driven and quantum-ready cybersecurity technologies. By empowering Canadian innovators through security institutions can ignite a new era of cyber defense leadership, technological sovereignty, and economic strength on the world stage.

Project Collaborators

• CYBERECO (Quebec)

Quebec-based cybersecurity accelerator supporting go-to-market strategy, ecosystem development, and Canadian market commercialization activities.

• SIMNET (Ontario)

Provides sovereign German private cloud infrastructure, high-performance event bandwidth, and international hosting capacity for CYBERPASS™ deployments across Europe.

• Blueteam GmbH (Germany)

Exclusive CYBERPASS™ reseller for Germany. Leads German market commercialization, CISO/CTO outreach, Healthcare sector deployments, and German-language support.



From left to right: BlueTeam (German Partner), The Hon. Evan Solomon, Michel Bourque, Jim Campbell, SIMNET (Photo taken at The Canadian Embassy, Paris).



From left to right: BlueTeam partner Matthias Kosiowski, M. Thomas Jaronbek, Federal Ministry for Digital and State Modernisation, Cyberdefense ai, Simnet and cyberdefense.ai (Photo taken at The Vivattech 2025)



Acknowledgements

This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN)
Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC)



Security Patch-related Regressions in Software Supply Chain

Lorenzo De Carli, Associate Professor, University of Calgary

Lorenzo De Carli
lorenzo.decarli@ucalgary.ca

Thanoshan Vijayanandan
thanoshan.vijayanand@ucalgary.ca

Project Description

Open-source software packages are widely used [1], but **security patches** can unintentionally break downstream projects that depend on them.

This project investigates these **security patch** related issues (for example, **regressions**) in the software supply chain

- Focus: detecting and mitigating regressions caused by npm security patches in downstream projects
- Goal: build a regression dataset, characterize risks, and develop automatic detection tools
- Team: researchers at University of Calgary and University of Kansas
- Context: growing reliance on open-source ecosystems creates new software security challenges for organizations adopting security patches

Project Collaborators

- Drew Davidson (University of Kansas)
- Dominic Tassio (University of Kansas)
- Thanoshan Vijayanandan (University of Calgary)

Budget & Method

Project funding and execution approach:

- NCC contribution: **CAD \$470K**
- Method: mining npm GitHub Security Advisories and npm fix commits to build a regression dataset. Sandbox testing to detect regressions automatically before adopting security patches

Known Regression Incident

- **CVE-2025-27556** fix introduced a 2048-character URL limit to prevent denial-of-service attacks [5]
- This change broke authentication redirects and third-party service URLs (e.g., Amazon S3) that exceed the limit, causing redirect and authentication failures

Current Progress

- Conducting literature review
- Constructing a npm security patch related regressions dataset

Future Exploration

- Characterizing downstream regressions
- Develop guidelines and best practices for maintainers to minimize regression risks when releasing security patches
- Automatically detecting regression risks before security patch adoption
- Evaluating regression mitigation strategies
- Studying the impact of delayed patch integration

Motivation

- Prior research shows that developers often avoid dependency updates due to concerns about **regression risks**, even when vulnerabilities are known [2]
- Packages under active development rarely dedicate separate releases for **security patches**, often bundling them with unrelated code changes [3,4]
- Package maintainers may not strictly follow semantic versioning when releasing breaking changes
- Although previous studies acknowledge that **security releases** can introduce **regression risks**, there is limited research systematically analyzing these issues in downstream projects

Reference

- [1] R. K. Vaidya, L. De Carli, D. Davidson, and V. Rastogi, "Security issues in language-based software ecosystems," arXiv preprint arXiv:1903.02613, 2019.
- [2] Pashchenko et al. "A qualitative study of dependency management and its security implications." CCS 2020
- [3] B. Chinthanet, R. G. Kula, S. McIntosh, T. Ishio, A. Ihara, and K. Matsumoto, "Lags in the release, adoption, and propagation of npm vulnerability fixes," Empirical Software Engineering, vol. 26, no. 3, p. 47, 2021.
- [4] N. Imtiaz, A. Khanom, and L. Williams, "Open or sneaky? fast or slow? light or heavy?: Investigating security releases of open source packages," IEEE Transactions on Software Engineering, vol. 49, no. 4, pp. 1540–1560, 2022.
- [5] Django Software Foundation, "Ticket #36743: Max URL length of 2048 is too conservative for redirect targets." [Online]. Available: <https://code.djangoproject.com/ticket/36743>

Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).

Privacy





Designing a scalable oblivious database

Sujaya Maiyya, Florian Kerschbaum
University of Waterloo

UNIVERSITY OF
WATERLOO



DAVID R. CHERITON SCHOOL
OF COMPUTER SCIENCE

Project Description

- This project builds scalable, privacy-preserving databases for secure cloud use in sensitive sectors like healthcare and finance.
- It tackles the limitations of existing solutions that either suffer from performance bottlenecks or leak sensitive information through access patterns.
- Our goals include:
 - Building an oblivious high-throughput database
 - Supporting complex analytical queries on encrypted data, and
 - Enabling private search over vector databases.
- The work addresses the need for secure, cloud-based data processing.

Project Collaborators

- This project is led by PI Dr. Maiyya and co-PI Florian Kerschbaum from the University of Waterloo.
- The team also includes external collaborators for requirement gathering. This includes RBC and Airbus.
- AWS is providing the cloud-credits to test the systems we aim to develop through this proposal.

Budget & Method

- The NCC contribution for this 4-year project is \$295,000 CAD
- The matching contribution for the project is \$295,000 CAD
- The project is being executed through a combination of systems design, theoretical analysis, and practical implementation.
- We are developing open-source prototypes, conducting performance evaluations on our on-campus cluster, and validating real-world relevance through ongoing collaboration with industry partners.

Current Progress

- Identified four scalable oblivious systems, noting limitations such as hardware dependency and lack of scalability; our design is hardware-agnostic and scalable.
- Explored a multi-layer architecture that integrates diverse oblivious techniques and scales securely with client demand.
- Published 4 top-tier conference papers: 3 in USENIX Security and 1 in VLDB in 2025-2026 timeframe.

Future Exploration

We aim to continue exploring the project in the following ways:

- Design a scalable oblivious data system that caters to highly skewed real-world workloads with minimal overhead over plaintext stores.
- Integrate multiple obliviousness techniques within a unified, tunable framework.
- Extend support to complex queries and encrypted vector data for modern applications like analytics and LLMs.
- Strengthen industry collaborations to guide development and validate the system in real-world environments.

Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).



This project was made possible in part through the support of the University of Waterloo Faculty of Mathematics

Project Description

- Augmented (AR), virtual (VR), and mixed (MR) reality applications are burgeoning
- In virtual environments, it is impossible to know who is wearing the head-mounted display (HMD), leading to authentication and access control issues
- But... HMDs are packed with multimodal sensors!



- Research question #1:** Can we utilize HMD sensors to identify the user, their age, biological sex, and/or other demographic details? If so, can this be done in a secure privacy-preserving manner?
- Research question #2:** Are there new sensors we can integrate to improve authentication performance?

Project Collaborators

Pan-Canadian, interdisciplinary research team from Ontario, Quebec, and British Columbia

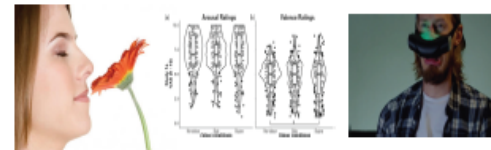
- Beam Me Up Augmented Intelligence:** VR healthcare platform for dementia patients
- In Virtuo:** VR platform for cyberpsychology sessions
- Keptics:** VR headset instrumentation for research
- CoLAB Numérique:** hyper-realistic human digital twins
- Digital Trust Canada:** digital credentials and trust
- MYND Therapeutics:** AR platform for chronic disease management
- INRS-UQO Joint Research Centre on Cybersecurity and Digital Trust:** graduate student training

Budget & Method

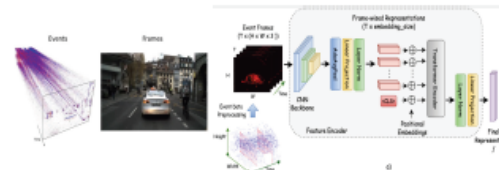
- Four years "Spearhead R&D" project
- First two years involve preparation of literature reviews, and conduct experiments with public HMD datasets
 - Build multimodal models for authentication and user identification, as well as models to predict user age, biological sex, and other attributes
 - Implement large AI models and test different AI model compression methods
 - Explore advantages of blockchain solutions
- Third year: collect first-of-its-kind data (based on obtained insights) to build final authentication and access control methods
- Last year to test methods on partner platforms
- Budget: \$500,000 (NCC) to cover student scholarships and travel to conferences, plus \$200k+ in partner time to attend meetings and provide advice, as well as a scholarship for multiple PhD students
- Six graduate students from INRS and three from University of Waterloo are involved

Current Progress

- Literature review → Advanced Intelligent Systems, 2026.
- Initial experiments performed with age and biological sex prediction and user identification using EEG (electroencephalography) signals collected during VR experiments
 - Deep learning methods outperform classical machine learning methods, but not by much
 - Results significantly better than chance
 - Published in IEEE SMC Conference, Oct. 2025
- Experiments with speech and EEG foundations models are showing very promising results
 - Published in IEEE Conference on AI, May 2026
 - Three journal papers under preparation
 - Speech also shown to predict speaker height
- Multisensory vs conventional VR — adding smells boosts user identification accuracy by 20%!
 - Results published at CVPR, June 2026



- New neuromorphic event camera shown to better track subtle eye movements, which are crucial for authentication
 - Outperformed three state-of-the-art methods
 - Published in IEEE Conference on AI, May 2026



Future Explorations

- Compression of multimodal foundation models
- Vulnerability of models to adversarial attacks
- Extend multisensory work to demographics prediction
- Prepare ethics documents for Year 3 data collection
- Quantum computing vs blockchain

Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN). Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC)



Secure Genomics Data Processing

Sujaya Maiyya
University of Waterloo



Project Description

The project aims to develop a secure infrastructure to process **encrypted genomic data** using **Trusted Execution Environments (TEEs)**, protecting privacy during both storage and computation.

High-Level Goals & Milestones:

- Automate the conversion of genome-processing libraries to TEE-executable code
- Survey and integrate memory-oblivious techniques to prevent side-channel attacks
- Design an **oblivious memory controller** for secure and efficient execution

Context and Landscape:

- It responds to real-world privacy failures (e.g., **23andMe data breach**) and addresses the limitations of anonymization and access control
- Supports the future of **personalized medicine** by making secure genome processing feasible and scalable

Project Collaborators

- This project is led by PI Dr. Maiyya from the University of Waterloo.
- The team will include 2 graduate and 2 undergraduate students.

Budget & Method

- The NCC contribution for this 2-year project is \$129,900 CAD
- The matching contribution for the project is \$20,000 CAD
- The project is being executed with tools and system development components combining systems engineering, security analysis, and bioinformatics expertise
- The project conducts hands-on experimentation using TEEs (e.g., Intel SGX/AMD SEV) to validate performance, usability, and security

Current Progress

- Assessed emerging TEEs (Intel TDX, AMD SEV) and found VM-based TEEs simplify secure execution of monolithic bioinformatics libraries.
- Insights from tool comparison and expert consultations guided automation of secure transformation pipelines in the next phase.
- Surveyed oblivious memory controller techniques to analyze the fitness for genomics data processing pipelines and use cases.

Future Exploration

We aim to continue exploring the project in the following ways:

- Design and implement memory-oblivious techniques and an oblivious memory controller to prevent side-channel attacks during genomic data processing.
- Expand secure processing framework to support diverse genomics applications and deploy on emerging TEE platforms like Intel TDX and AMD SEV SNP.
- Collaborate with bioinformatic researchers to validate solutions in real-world settings.
- Build a visualization scheme to communicate the privacy findings to a lay people, genomics researchers, and policy makers.

Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).



This project was made possible in part through the support of the University of Waterloo Faculty of Mathematics

Preserving Relationship Privacy in Large Networks

Keval Vora
keval@cs.sfu.ca, Simon Fraser University



<https://pragma.cs.sfu.ca/>

Project Description

- Recent advances permit learning intricate and complex relationships between entities.
- Preserving sensitive information like participation in certain communities or group-level interactions has become important.

Goal: Enable privacy at the level of complex and transitive interrelationships.

Approach:

- Model privacy constraints at subgraph-level.
- Capture interdependence between individual data-points, relationships in their broader communities, and across the entire network.
- Leverage the model constraints to generate privacy-preserving solutions according to scenario requirements.

Overview of Milestones:

- Benchmark scenarios with various relationship-level privacy threats.
- Build threat mitigation components for various identified scenarios.
- Evaluate and release mitigation components.
- Identify potential industry partnerships.

Team:

- Spearhead project undertaken by researchers from Simon Fraser University:
 - PI: Dr. Keval Vora
 - Co-PI: Dr. Anders Miltner
 - PhD Student: Adam Tan
 - PhD Student: Ziyi Yan
 - MSc Student: Nazanin Yousefian

Budget and Method

Current Budget: \$500,000 (Spearhead Project)

- Wages & Salaries: \$350,000
- Equipment, Travel & Outreach: \$75,000
- Indirect Costs: \$75,000

Methods:

- Investigate graphs and identify common relationship-level privacy scenarios.
- Develop a formal notion of relationship-level privacy for such scenarios.
- Develop algorithms that guarantee relationship-level privacy is preserved.

Current Progress

- Identified benchmark suites with various characteristics to help guide the privacy requirements across scenarios.
 - Includes schema-based data graphs.
- Currently designing the k-hop centric and community-centric threat mitigation components (underpin privacy-preservation for graph analysis).
- Example Queries:
 - Average number of smoking friends or friend pairs



- Releasing actual participation may impact adversely for individuals (e.g., health insurance premiums).
- Currently identifying how correlated a priori information and known data characteristics can be leveraged to enhance privacy in practice.

Further Exploration

- Published a paper (SIGMOD SeQureDB 2026) on privately estimating practical graph dataset characteristics for downstream analytics/learning.
- Plan to expand to k-hop centric and community-centric threat mitigation components.
 - On track with milestones 2 and 3
- Subsequently, explore different use cases.
- Explore potential collaborations to capture their scenarios and deploy solutions.
- Publish papers in top conference/publication venues demonstrating our findings.

Potential future exploration (beyond scope):

- Guidelines and best practices for preserving relationship privacy to potentially inform policies for sensitive data protection.
- A framework to automatically generate threat mitigation solutions, and to certify privacy guarantees in human-developed solutions.
- A framework for porting algorithms that preserve one notion of relationship privacy to versions that preserve different notions of privacy.

Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).

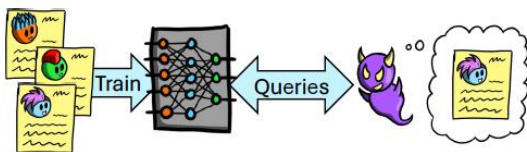


Novel Methods for Quantifying and Improving PRIVACY in Machine Learning

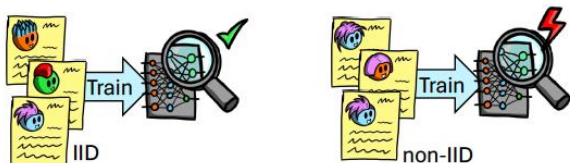
Simon Oya, Karthik Pattabiraman, Julia Rubin (UBC)

Project Description

Machine learning models leak privacy-sensitive information about their training data!



Current approaches to **measure** and **provide** privacy assume data samples are independent (IID). This is not true in many real-world scenarios (non-IID).



How do we quantify and provide privacy in this non-IID setting?

Team

Faculty members from the ECE department at UBC:

- Simon Oya (simon.oya@ubc.ca)
- Julia Rubin (juliarubin@gmail.com)
- Karthik Pattabiraman (karthikp@ece.ubc.ca)



Budget & Method

Spearhead project. Research conducted at UBC.

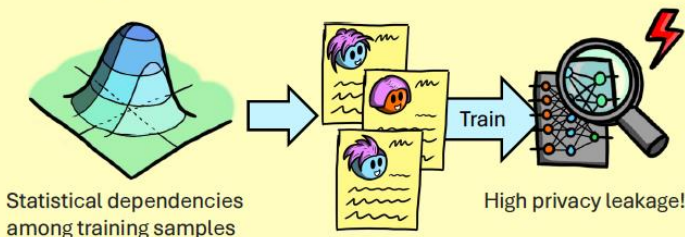
Start in **September 2025**.

Total budget 495,000 CAD from NCC.

Our research includes both **theoretical privacy analyses** as well as **empirical** evaluations of privacy attacks and defenses.

Project Exploration

How do we quantify and prevent privacy leakage for realistic data distributions?



Reach out to potential partners (O5)



Reach out for partners interested in understanding the privacy of their models. Conditional on their approval, apply our auditing tools to their applications.

Understanding realistic data dependencies (O1)

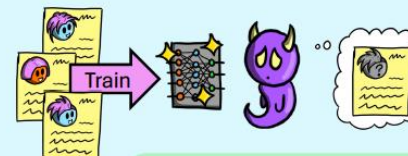


What are common sources of data dependencies in real datasets? How do we model those dependencies?

Examples:

- spatio-temporal dependencies (time series, location data)
- near-duplicates and augmentation
- hierarchical (hospitals, schools, etc.)
- social graphs (friends, family members).

Develop defense mechanisms under data dependencies (O4)



Can we leverage our models for data dependencies (O1) to **strengthen defenses** (differential privacy, empirical defenses) against attacks in non-IID settings?

Develop new privacy auditing tools



Theoretical (O2)

Differential privacy

Differential privacy (the most common provable privacy framework) does not guarantee protection in non-IID settings. We will study how to extend it to non-IID settings.

Empirical (O3)

Inference attacks

Inference attacks (e.g., membership inference) are mainly evaluated in IID settings. We will study attacks in non-IID settings.

Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).

Project Description

This project develops a privacy-preserving software framework to protect children's personal data in Large Language Models (LLM) applications. It provides data security, compliance with laws like PIPEDA and COPPA, and includes real-time monitoring, consent management, encryption, and audit logging—built on a decentralized, blockchain-based system. The project will empower Canadian parents to have greater control over the collection and utilization of their children's personal data within LLM-based platforms.

Project Focus

Our project addresses privacy risks for children using LLMs, supports Canadian schools and child-focused services in adopting AI tools, and develops privacy-preserving policies, technologies, and legal guidance. It ultimately promotes the ethical and secure use of AI in contexts involving children.

High-Level Goals & Milestones

- Phase 1: Propose privacy guidelines aligned with PIPEDA, COPPA;
- Phase 2: Identify data risks and enhance parental consent.
- Phase 3: Build secure data storage and pilot tools and develop Consent Management System for Canadian families.

Context & Landscape

With the growing use of LLMs in Canadian education and child-focused services, existing privacy laws show gaps in adequately protecting children's data. This project addresses an urgent need for transparent and verifiable consent mechanisms while enabling the monitoring of data practices and processing operations in LLM-based applications.

Current Progress

WP1 – Transparent Consent Management

Developed a blockchain-enabled consent management framework for child-oriented LLM applications. Designed and implemented an auditable privacy notice interface with integrated age verification and smart contract support. Completed Deliverables D1.1 and D1.2 and achieved planned TRL 1-2 milestones.

WP2 – Privacy-by-Design Framework

Conducted privacy threat and risk analysis for children's data in LLM applications.

Developed a privacy-by-design framework mapping legal privacy principles to different stages of LLM data processing.

Learned that privacy requirements must be embedded directly into AI data pipelines rather than added afterward.

WP3 – Monitoring & Accountability

Developed a prototype monitoring framework integrating blockchain and Trusted Execution Environments (TEE).

Implemented an event-driven accountability mechanism to support transparent and verifiable monitoring of children's data processing.

Initial evaluations showed the feasibility of combining secure hardware and blockchain for accountable AI monitoring.

Research Outputs & Impact

Published and presented research at leading international conferences including:

- International Conference on Risks and Security of Internet and Systems
 - IEEE/ACM International Conference on Utility and Cloud Computing
- Additional journal and conference papers are currently under review.

Project Evolution

The project evolved from initial consent management research toward a broader accountability and monitoring framework for privacy-preserving LLM systems. Figure 1 shows an abstract model of the framework relying on events generated as evidence. Current work focuses on automated compliance verification and trustworthy AI governance for children apps.

Acknowledgements

This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (GCN).
Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RCC).



Budget & Method

The total budget requested for the project is \$88,800 CAD, with the full amount contributed by NCC. Matching funds will be provided through in-kind supervision and institutional support. The budget includes \$74,000 CAD allocated for student salaries and \$14,800 CAD for indirect costs. All students involved in the project will dedicate 100% of their research time. The project will be executed over 24 months in three phases:

Phase 1 (Months 1-8) will focus on developing policy guidelines and identifying international best practices;

Phase 2 (Months 9-15) will address privacy threat analysis and consent management;

Phase 3 (Months 16-24) will concentrate on secure and trusted data handling.

Project Collaborators

For this project, we hired two PhD students, one master's student and one undergraduate student. One PhD student is working on technical solutions for both consent management and monitoring tool. The undergraduate student is directly working with the PhD student for the practical implementation. The other PhD leads the threat models and privacy by design scheme and collaborates with the master student.

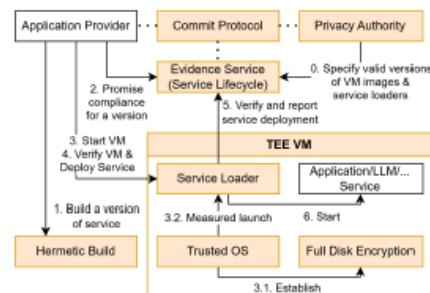


Fig. 1: System architecture for trusted evidence service and accountable monitoring [1]

Future Exploration

Future work will focus on enhancing the proposed framework to support real-time and large-scale privacy compliance monitoring in LLM-based systems. The project aims to improve the transparency and explainability of AI-driven consent and auditing mechanisms, enabling organizations to better understand how personal data is collected, processed, stored, and shared within LLM applications. In addition, future research will investigate more advanced automated compliance verification techniques using machine learning and blockchain technologies to strengthen accountability and trustworthiness. The framework will also be evaluated in broader real-world environments, particularly in applications involving children's data and sensitive personal information. Moreover, it will extend its support for more international privacy regulations and evolving AI governance standards.

Reference

- [1] C. Zhou, M. Barati, and N. Kahani, A Privacy Compliance Framework with Forensic Evidence for Child-Facing Large Language Model-Based Applications, 23rd Annual International Conference on Privacy, Security, and Trust, 2026, [submitted]



Secure Healthcare Data Federation through Generative Access Control

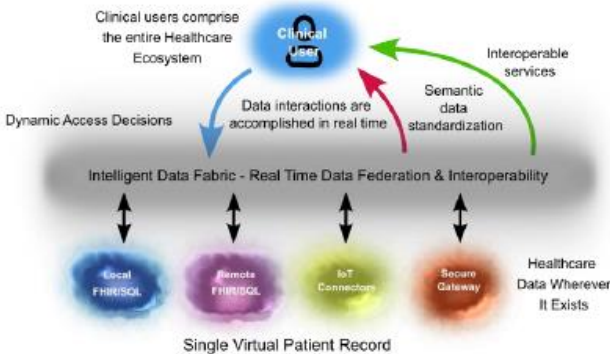
Bryan Simmons Otekha Health Corporation bryan.simmons@otekha.com



Project Description

Data Silos are bad for Healthcare

- ✗ Data silos in healthcare severely harm patient outcomes by creating fragmented records, leading to misdiagnoses, delayed treatments, repeated tests, and medication errors
- ✗ Patients can't access their own information, limiting their ability to drive their own healthcare
- ✗ Silos limit research and the use of AI which is driven by large amounts of data



Our work aims to solve one of the hardest problems in Healthcare – how to create a Pan-Canadian real-time view of each person's complete healthcare record.

We will achieve this through a novel, dynamic and generative access control (GenerAC™)

Current Progress

- ✓ Otekha is supporting academic research across four (4) Canadian Universities through Mitacs grants that will support eight (8) students over the term of this project
- ✓ We are working with technology vendors in the design of a high performance cluster to evaluate the performance and scalability characteristics of the software technology being developed
- ✓ Discussions are underway with Provincial health ministries to include Provincial healthcare staff in how real-time data federation and interoperability can be used in their respective jurisdictions

Future Exploration

- ❖ Research into the application of AI in the agentic management and defense of a High-Performance Computing platforms
- ❖ Realizing a US DoD Zero Trust model that incorporates GenerAC™ and Post Quantum Cryptography in a High-Performance Computing platform
- ❖ Application of GenerAC™ to address the security challenges of AI Model Context Protocol (MCP)

Project Collaborators

Prof. Natalia Stakhanova – University of Saskatchewan

Adaptations of NIST NGAC for Data Federation and Interoperability

Prof. Karim Keshavjee – University of Toronto

Health Data Governance Through Smart Contracts
Methods for Semantic Consistency in a Real-time Federated and Interoperable Healthcare Platform

Prof. Plinio Morita – University of Waterloo

Personal Data Governance Through Digital Consents
Methods for Semantic Consistency in a Real-time Federated and Interoperable Healthcare Platform

Prof. Fatemeh Khoda Parast – University of New Brunswick

Sovereign Cloud Architecture, Performance and Scalability Considerations for National Scale Data Federation and Interoperability

Budget and Method

This research project was made possible through a \$2.38M grant from the National Cybersecurity Consortium (NCC)

Research methods include:

- Requirements gathering from key stakeholders (5 > of Hospitals, Family Medicine Clinics, and 25 > members of the public)
- Matching stakeholder requirements to designed functionality
- Mapping requirements to NIST NGAC framework to ensure all requirements are managed appropriately



Acknowledgements

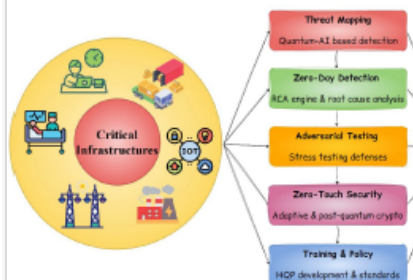
This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN)
Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RiC)

Quantum





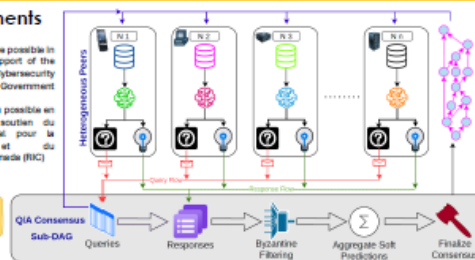
Project Description



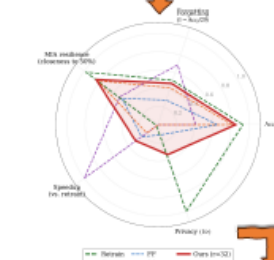
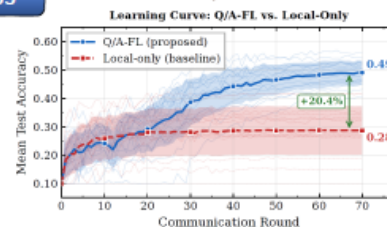
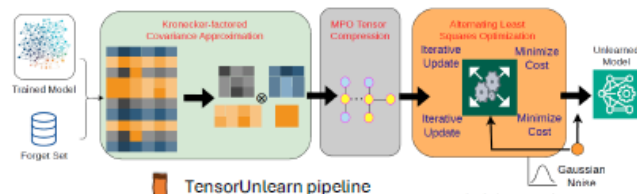
Acknowledgements

This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSC). Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RSC).

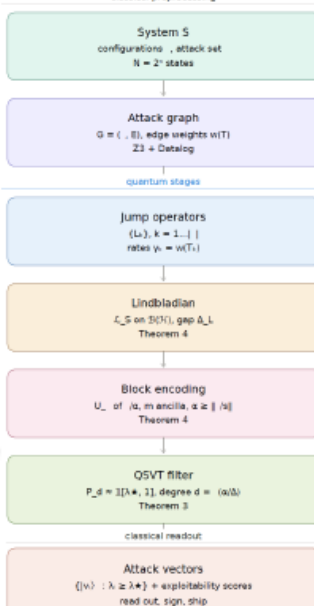
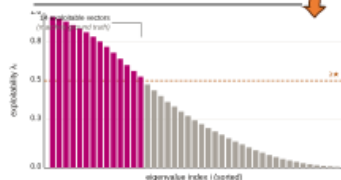
CI Test Bed
UCalgary Smart CPS Lab



Current Progress



Setting	Method	Acc. ↑	Acc. ↓	MIA	Time	ϵ
CIFAR-100 [5] = 30	Retrain	94.3	9.8	50.2	47m	0
	GA	89.1	6.2	54.8	35s	-
	FF	91.5	14.3	55.1	4.2m	0.7
	SCUB	93.1	11.5	51.8	6.3m	-
	KFAC-only	93.0	11.2	52.4	3.5m	3.2
	Ours (r=10)	93.2	11.0	52.1	2.4m	3.3
CIFAR-100 [5] = 50	Ours (r=32)	93.5	10.5	51.6	3.1m	2.9
	Retrain	71.8	0.8	50.1	38m	0
	GA	65.2	0.3	56.4	28s	-
	FF	68.4	3.1	55.8	3.8m	11.2
	SCUB	70.5	1.4	52.1	5.4m	-
	Ours (r=32)	71.0	3.1	51.4	2.8m	3.7



Project Collaborators

This project brings together a team of esteemed researchers from leading Canadian institutions and industry. Dr. Hadis Karimipour (Project Lead, University of Calgary) and Dr. Israat Haque (Co-Lead, Dalhousie University) guide the overall vision and execution. Contributing their expertise as investigators are Dr. Marina Gavrilova and Dr. Julien Ross, representing the University of Calgary and Dalhousie University respectively, alongside Dr. Pierre-Luc Dallaire-Demers from Pauli Group Inc.

Budget & Method

The project is being executed through a strategic allocation of resources, focusing on two key components: human expertise and computational infrastructure. The allocated budget is utilized primarily for **staff salaries**, ensuring skilled professionals are engaged in critical project tasks. Additionally, a significant portion is invested in acquiring **high-performance computing (HPC)** systems, which are essential for processing large datasets and running complex simulations efficiently.

Future Exploration

Advance quantum-AI-driven critical infrastructure protection through zero-day threat detection, adversarial stress testing, and Zero-Touch security deployment across ICS/OT environments, validated on real-world test beds.

Post Quantum Resilience of Cyber-Physical Power Systems

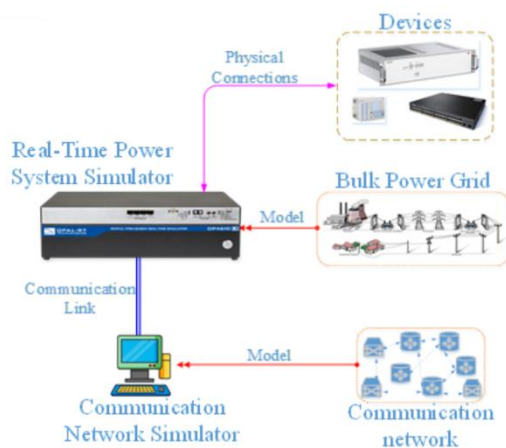
Project Lead: Atefeh (Atty) Mashatan, Toronto Metropolitan University, amashatan@torontomu.ca

Co-Lead: Reza Arani, Toronto Metropolitan University, marani@torontomu.ca



Project Description

- Cryptographically-relevant Quantum computers will weaken today's cryptography, creating future risks for power-grid communications and threatening the availability of critical infrastructure.
- This project evaluates recently standardized post-quantum cryptography (PQC) for real-time power-system protocols such as GOOSE/SV, R-GOOSE/R-SV and MMS.
- The goal is to secure critical grid operations against the threat of quantum computing without sacrificing latency, availability or reliability.
- Using realistic co-simulation and hardware-in-the-loop testing, the project builds practical evidence for utilities and manufacturers.



Real-Time Co-Simulation Platform

Budget

- NCC contribution \$500,000.
- Matching support: \$35,000 + \$40,500 anticipated in-kind.
- ABB Canada: protection equipment/software, including SSC600.
- Hydro Quebec: expert guidance on power-system cybersecurity, communication networks, and co-simulation.

Method

- Create a safe "digital twin" of the grid: We will recreate power-grid operations and communications in a realistic lab environment, including commercial protection devices used by utilities.
- Simulate cyberattacks safely: This lab setup allows us to study how cyberattacks could affect the grid without exposing any real infrastructure to risk.
- Test quantum-safe security tools: We will evaluate selected post-quantum cryptography methods to see whether they can protect grid communications while still meeting strict speed and reliability requirements.
- Guide real-world adoption: The results will help identify practical ways for utilities to move toward quantum-safe cybersecurity.

Current Progress

- Project has recently started its Q2.
- Our existing TMU cyber-physical testbed provides the foundation for wide-area and inter-substation studies.
- Early work with Hydro Quebec researchers identified quantum-related vulnerabilities in substation automation.
- Testbed upgrades and partner equipment integration will support realistic PQC evaluation.

Future Exploration

- Identify PQC options/parameters that meet OT constraints for latency, computation and availability.
- Develop hybrid migration strategies where classical and quantum-safe devices coexist.
- Produce a utility-oriented roadmap for transition to quantum-safe power-system cybersecurity.
- Project activities extend analysis from intra-substation protocols to wide-area protection/control communications.
- Expand the platform for quantum key distribution (QKD) studies, broader OT cybersecurity testing and future industry collaboration.

Project Collaborators

- Toronto Metropolitan University: Cybersecurity Research Lab & SecGrid Lab
- Leads: Atefeh (Atty) Mashatan and Reza Arani
- Partners: ABB Canada; Hydro-Québec / IREQ
- HQP: 1 PhD student and 2 PDFs

Acknowledgements



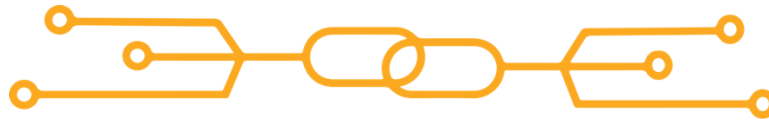
This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).

Additional thanks to Toronto Metropolitan University, ABB Canada, Hydro-Québec / IREQ, and project HQP.

CYBERSECURITY
RESEARCH LAB



Secure AI



Adaptive AI Firewall Specializing in the Protection of AI Models, Critical Infrastructure, Systems, and Agents

Apurva Narayan, Western University, apurva.narayan@uwo.ca



Project Description

The Adaptive AI Firewall (AAF) project creates a dynamic multi-agent cybersecurity system that continuously adapts to protect complex AI-driven infrastructure against evolving threats. Key goals include developing advanced learning mechanisms, filing patents, commercializing products, and fostering global collaborations. The team comprises academic and industry experts dedicated to advancing AI cybersecurity solutions.

Development of Multi-Agent AI System: Establish an architecture where multiple specialized security agents dynamically cooperate, communicate, and share threat intelligence.

Continuous Learning Capabilities: Implement a robust learning mechanism enabling the firewall to adapt to novel threats and continuously improve its defense strategies.

Academic Excellence: Train 3 PhD and 2 Masters students specializing in adversarial machine learning, secure multi-agent systems, and AI-driven threat intelligence.

Global Collaboration Network: Form strategic partnerships with national institutions (UBC, Waterloo, Western, Queens) and international organizations, creating a robust global cybersecurity intelligence-sharing community.

Budget & Method

Project Method and Execution:

- Employing an agile methodology focusing on iterative design, testing, and refinement of multi-agent cybersecurity systems.
- Leveraging continuous adversarial training and specialized task-focused AI models for adaptive threat detection.

Project Budget:

NCC Contribution: \$500,000 CAD (student support, IP costs, commercialization, partnerships, dissemination, equipment).

Anticipated Match (Palitronica): \$592,000 CAD in-kind (engineering, data science, marketing, strategic expertise).

Current Progress

Project Awarded

(2 PhD, 1 Research Associate, 3 UGs Onboarded)

AI-based Security Verification – Utilizing LLMs to Generate Tailored Security Tests

- Papers published at ESCAR 2025, AAMAS 2025, KDD 2026

- Validation in Progress with Palitronica Inc.
- Technology is advancing fast, AI Agents will play a key role

Future Exploration

Conduct comprehensive prototype testing in simulated real-world environments.

Expand collaborations with global cybersecurity firms and institutions for enriched threat intelligence sharing.

Explore scalability in IoT and edge computing ecosystems to broaden the project's applicability.

Secure additional funding and strategic partnerships to support large-scale deployment and continuous R&D.



Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).

Project Collaborators



Self-Healing AI Security via Autonomous Patch Generation & LLM Autovaccination

Fattane Zarrinkalam, University of Guelph, fzarrink@uoguelph.ca



Project Description

• Project focus

This project develops self-healing AI security methods to protect LLM-based systems from evolving cyber threats, including prompt injection, adversarial attacks, knowledge poisoning, and data leakage.

• Context and need

LLMs, RAG, and GraphRAG systems are increasingly used in critical sectors. However, current defenses are often static, reactive, and limited against fast-changing attacks.

• Goals and milestones

- Develop threat models for LLM, RAG, and GraphRAG security risks.
- Explore LLM AutoVaccination, autonomous patching, and repair mechanisms.
- Build real-time monitoring and adversarial red-teaming methods.
- Integrate self-healing components into a unified AI security framework.
- Evaluate the framework using benchmarks and realistic attack scenarios.

Project Collaborators

- **Fattane Zarrinkalam**
 - University of Guelph, Lead
- **Ali Dehghantanha**
 - University of Guelph, Co-Lead
- **Benjamin C. M. Fung**
 - McGill University, Investigator
- **Natalia Stakhanova**
 - University of Saskatchewan, Investigator
- **Frank Rudzicz**
 - Dalhousie University, Investigator

Budget & Method

• Budget

- NCC Grant: \$182,671 CAD
- Matching contributions: \$222,325 CAD
- Total project cost: \$364,996 CAD

• Project method

The project follows a staged R&D approach to investigate security risks in LLM-based systems and develop self-healing defense mechanisms. The work includes threat modeling, LLM AutoVaccination, autonomous patch generation, real-time threat detection, and adversarial red-teaming.

Current Progress

• Hop-wise repair for poisoned GraphRAG

- A GraphRAG defense was developed to monitor reasoning steps, identify poisoned graph elements, and repair the retrieved subgraph before answer generation.
- *Defense Against Knowledge Poisoning Attack on GraphRAG*, **ACL 2026**.

• Cross-encoder-based RAG protection

- A RAG defense method was introduced to use cross-encoder reranker signals for detecting poisoned content, localizing suspicious chunks, and replacing them before answer generation.
- *Defending RAG Against Knowledge Poisoning Using Cross-Encoder Activation Signals*, **Canadian AI 2026**.

• Resource-aware RAG repair

- A practical RAG repair method was proposed to diagnose factual errors using observable signals and select corrective actions under latency and compute constraints.
- *Diagnosing and Repairing Factual Errors in RAG under Budget Constraints*, **Canadian AI 2026**.

Future Exploration

• Broaden self-healing AI security approaches

The next phase will continue exploring different self-healing strategies for LLMs, RAG, and GraphRAG, including autonomous detection, diagnosis, repair, and recovery from attacks.

• Advance RAG and GraphRAG protection

Future work will further investigate defenses against poisoned, missing, or misleading evidence, with a focus on repairing retrieved contexts, and corrupted graph structures

• Explore adaptive LLM defense mechanisms

The project will examine how LLMs can improve resilience through methods such as self-adversarial training, autonomous patching, safety monitoring, and feedback-driven refinement.

• Develop unified evaluation methods

Future work will define consistent evaluation metrics and benchmarks to compare self-healing methods.

• Expand testing and collaboration

Further validation is needed across larger datasets, stronger attack scenarios, and real-world environments. New collaborations with cybersecurity, public-sector, and industry partners will support practical evaluation.

Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).

We also gratefully acknowledge 3Tenets Consulting for their support and collaboration.



Cyber-Synthetic Risk

A Generative Multi-Agent Approach to Forecasting Advanced Cyberattack Impacts on Enterprise Ecosystems

Project Lead: Dr. Tahereh Hasani

Gordon S. Lang School of Business and Economics, University of Guelph |
htahereh@uoguelph.ca

- NCC Project ID: 2025-1630
- Project Lead: Dr. Tahereh Hasani
- Gordon S. Lang School of Business and Economics, University of Guelph
- Contact: htahereh@uoguelph.ca

Project Description

- Cyber-Synthetic Risk develops a self-evolving, AI-driven cybersecurity platform to forecast how advanced cyberattacks may affect enterprise ecosystems, including operations, data, reputation, and organizational resilience.
- The project advances from framework design to functional prototype development through five milestones: AI-enabled framework design, generative cyberattack simulation, multi-agent attacker-defender modelling, adaptive risk analytics, and final platform integration and validation.
- The project is led by Dr. Tahereh Hasani at the Gordon S. Lang School of Business and Economics, University of Guelph, with a cross-Canadian academic team and industry partners supporting technical development, use-case relevance, and real-world validation.
- As ransomware, zero-day exploits, and complex supply-chain threats continue to challenge organizations, this project moves beyond static cyber-risk models by using generative AI, multi-agent simulation, and real-time threat intelligence to support proactive cyber-risk decision-making.

Project Collaborators

- Academic team:
Dr. Tahereh Hasani, University of Guelph / Gordon S. Lang School of Business and Economics; Dr. Ali Dehghantanha, University of Guelph; Dr. Abbas Yazdinejad, University of Regina; Dr. Kuljeet Kaur, École de technologie supérieure (ÉTS); Dr. Saqib Hakak, University of New Brunswick; Dr. Gautam Srivastava, Brandon University
- Industry and public-sector partners:
Fortinet Canada; InCloud Security Inc.; Riskview Systems; Toronto Community Housing Corporation

Budget & Method

- NCC contribution: \$159,850; matching contributions: \$245,200; total project value: \$405,050.
- The project develops a self-evolving AI cybersecurity forecasting platform through five milestones: framework design, generative threat simulation, multi-agent modelling, adaptive risk analytics, and final integration/validation.
- The platform combines generative AI/GAN-based cyberattack scenario creation, multi-agent attacker-defender simulation, real-time threat intelligence, and operational data.
- Academic researchers build and integrate the platform, while industry and public-sector partners support use-case relevance, scenario realism, and prototype validation.

Current Progress

- Project initiation is underway, including milestone planning, team coordination, and alignment of research activities with the approved NCC project scope.
- Milestone 1 work has advanced through a targeted review of GAN-based cyber-threat generation, multi-agent simulation, and real-time threat-intelligence integration.
- The initial structure of the AI-driven cybersecurity forecasting framework has been defined, including core system components, scenario priorities, and technical requirements.
- Early planning is in place for the next phase: developing the generative cyber threat simulation engine and preparing partner-informed validation activities.

Future Exploration

- Next steps focus on building the generative cyber threat simulation engine, followed by multi-agent attacker-defender modelling and adaptive risk analytics.
- Continued partner engagement will be needed to validate realistic attack scenarios, operational assumptions, and prototype usefulness in real-world organizational settings.
- The project can expand through additional sector-specific pilots in areas such as public infrastructure, finance, healthcare, and enterprise cybersecurity.
- Future growth may include commercialization pathways, patent development, and a scalable decision-support platform for predictive cyber-risk management.

Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).

Lead unit: Gordon S. Lang School of Business and Economics, University of Guelph | Project ID: 2025-1630 | Contact: htahereh@uoguelph.ca



Project Description

- **Context:** Security of agent AI systems is a widespread and pressing issue
 - **36% of 3,984 agent skills** audited by Snyk contained security issues (source: <http://snyk.io/>).
 - **90+ organizations** attacked by malicious prompt injections reported in 2026 CrowdStrike Global Threat Report.
- **Goal:** framework for systematic assessment and assurance of agentic AI security
 - **cyber threat analysis and characterization** (pillar 1);
 - **security testing** (pillar 2);
 - **secure deployment** (pillar 3);
 - **security monitoring** (pillar 4).
- **Team:** collaborations between **software engineering and cybersecurity** experts.

Project Collaborators

- Polytechnique Montréal**
- Prof. Foutse Khomh
 - Prof. Mohammad Hamdaqa

- University of Waterloo**
- Prof. Yousra Aafer

Security Assessment and Assurance Framework for Agentic AI Systems			
Agentic AI System			
LLM Brain · Agents · Memory · Tools · Environment			
Pillar 1 Cyber Threat Analysis	Pillar 2 Security Testing	Pillar 3 Secure Deployment	Pillar 4 Security Monitoring
Threat Modeling Attack Surface Mapping Vuln. Characterization Risk Assessment	Benchmarking Verification & Validation Attack Simulation Red-Teaming	Sec-Aware Config Access Control Lifecycle Constraints Agent Sandboxing	Runtime Auditing Anomaly Detection Behavior Profiling Incident Response

Current Progress

Current progress:

- Started pillars 2 (testing) and 4 (monitoring):
 - literature and open-source agent/skill reviews;
 - experimental testing of agentic AI against direct/indirect prompt injections;
 - an SLR report on security-oriented observability of agentic AI;
 - categorized the impact of adversarial attacks on agentic AI.

Early findings:

- Latest agentic AI is typically post-trained with **security awareness**, but still suffers from adversarial attacks;
- **attacking skills** achieves a much higher success rate than direct prompt injections;
- observing the **trajectories** of agentic AI systems can reveal **risk indicators** out manifested in the output; such risk indicators can be leveraged to increase attack success rate.

Budget & Method

Budget:

- Planned for four full-time PhDs; currently one PhD and one master's work full-time on the project.

Source	NCC Grant	Matching	Total
Amount (3Y)	\$ 500 K CAD	\$ 189 K CAD	\$ 689 K CAD

Matching contribution is the form of salaries of the participating researchers.

Method:

- Each pillar: research -> prototype -> framework integration
- Weekly online sync-up meeting & annual report meeting



Acknowledgements

This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (GCN).
Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (GRC).
This project was also partially supported by Polytechnique Montréal and the University of Waterloo.
Ce projet a reçu le soutien partiel de Polytechnique Montréal et de l'Université de Waterloo.

Future Exploration

Next steps:

- Continue to work on the four pillars; onboard another two PhDs.
- Publishing research outcomes (papers, benchmark, and open-source framework).

Exploration:

- Look for industry/non-profit collaborations.
- Collaboration with enterprise agentic AI provider/user can help:
 - 1) understand better concerns of enterprise agentic AI,
 - 2) develop & evaluate framework with concrete cases.



Securing AI Agents Against Malicious or Vulnerable Tools

Meng Xu & Sihang Liu (Co-Leads), University of Waterloo
meng.xu.cs@uwaterloo.ca · sihangliu@uwaterloo.ca



Project Description

AI agents now act for us — booking trips or writing code. To do the work, an agent plugs in **external tools**, which often come from third parties.

- **Focus:** secure the tools an agent uses — the part outsiders supply.
- **Risk:** one malicious or buggy tool can leak private data or hijack the agent.
- **Goal:** find these weak spots automatically, then contain them with a sandbox built for AI agents.

Spearhead R&D · Apr 2025 – Mar 2028 · TRL 1 → 4

Project roadmap



Current Progress

Live discovery — “token injection” in submission to ACM CCS 2026

Inference frameworks insert hidden **special tokens** to control themselves. We found that ordinary user/tool text can be mistaken for these control tokens, letting a plain message reach the control path — and even crash the server.



Looks like an ordinary input or a careless mistake in input preparation, but can be exploited maliciously

Token injection: harmless user/tool text sneaks in as framework control commands

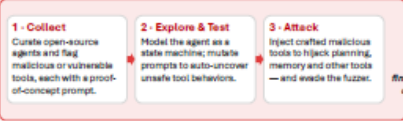
The chat-template guard was missing — so the plain message reached the control path.

Why it matters

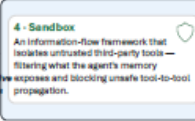
- A denial-of-service from one short, plain-text message, e.g., a simple and malformed tool reply
- Same trick can forge role markers and bend how the model behaves.
- The fix is a missing guard in the serving stack — exactly what our sandbox restores.

Budget & Method

OFFENSE · Red Team — break agents to learn how they fail



DEFENSE · Blue Team



Budget — CAD \$254,116, requested in full from the NCC (Spearhead).

Funds run over 3 years: \$172,500 by Mar 2027, \$103,500 across Years 2-3 to Mar 2029.

- **65% (\$180,000)** — graduate researchers: 3 students (PhD & thesis Master's) at \$30K/yr over 2 years.
- **35%** — conference travel & publication, LLM/cloud compute APIs, and 15% indirect cost.



Acknowledgements

This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (GCN). Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (GRC).

Project Collaborators

- 2 faculty members in U Waterloo
- 3 graduate researchers in AI & security

Seeking partners and collaborators:

Canadian AI startups & industry teams in finance, healthcare and enterprise software to co-test the defenses.

Tools may come from untrusted third parties

- One malicious or buggy tool can leak data or hijack the whole agent.
- Survey tool landscape
- Detect misuses
- Defense proactively

How widespread is it?



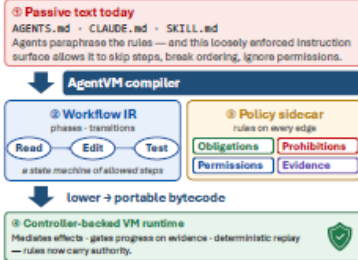
- 69% — no guard at all
- 31% — bypassable check only

Every framework we tested was exposed.



- We reported the issues to all inference frameworks we analyzed
- We confirmed the vLLM crash on a live deployment and reported it to the maintainers, the vulnerability has been patched.

Future Exploration



Differential Programming and Fully-Homomorphic Encryption at the Edge

Alaa Alameldeen, SIMON FRASER UNIVERSITY

Project Description

Artificial Intelligence (AI) models are becoming ubiquitous in applications such as healthcare, finance, robotics, fraud detection, and recommendation systems; but they require extensive training on private data, raising privacy and legal concerns. Fully-Homomorphic Encryption (FHE) enables secure, privacy-preserving computations on encrypted data that can be used in AI model training and inference. However, existing FHE frameworks incur prohibitive performance penalties, making real-world applications impractical.

This project advances privacy-preserving machine learning through accelerated homomorphic encryption and reduces processing time from hours to seconds, making interactive secure AI services viable for time-sensitive applications like medical diagnostics. This impacts use cases such as secure computations on private medical data, federated learning on edge devices, and protecting proprietary AI models.

The project designs a versatile, generalized hardware platform to support FHE computation using the novel approach of differential programming with practical processing-in-memory designs.

Budget & Method

NCC Contribution: \$1,000,000
Cash: \$6,000,000
In-kind: \$1,185,760
Total: \$8,185,760

Acknowledgements

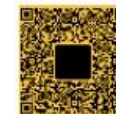


This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).



Protecting Democratic Discourse from GenAI Chatbots Posing as Humans

PI: Konstantin (Kosta) Beznosov, UBC, beznosov@ece.ubc.ca



Project Description

Problem addressed

- GenAI threatens democratic **representation, accountability, and trust** in Canada and around the world
- GenAI-driven **text chatbots posing as human interlocutors (TCPHI)** can undermine online democratic discourse
- Lack of understanding of **how much and why** Canadians are **vulnerable** to TCPHI attacks and **what can be done** about it

Objectives

1. **Empirically investigate vulnerabilities** of online discussion forums to TCPHI attacks
2. **Develop and empirically evaluate approaches to mitigating** TCPHI attacks

Context

- Interactive social media forums:
- Discussion groups on messaging platforms:
- Other public forums:



Project at a Glance

- Type: R&D Spearhead
- Start date: December 2025
- Length: 3 years, 4 months
- Budget: \$500,000
- Host organization: UBC



Current Progress

(RQ1) Measure how vulnerable Canadians are:

- Discussion forum prototype
- Human-imitating chatbot participating in the discussion forum
- Inventory of vulnerabilities of humans to AI artefacts.



Project Leads



Prof. Kosta Beznosov
ECE, UBC

- Usable Privacy and Security
- Systems Security



Prof. Cristina Conati
CS, UBC

- Artificial Intelligence & Machine Learning
- Human-Computer Interaction
- Human-AI Interaction

Method

Empirically investigate vulnerabilities

1. Measure how vulnerable Canadians are
2. Empirically determine vulnerability predictors

Develop and empirically evaluate mitigations

1. Automated vulnerability estimation
2. Interventions for reducing vulnerability

Future Exploration

(RQ2) Determine factors that predict user vulnerability.

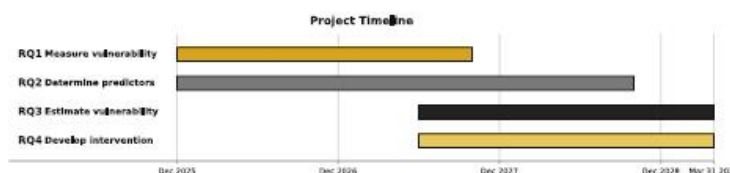
(RQ3) Develop ways to estimate the degree of individual user's vulnerability.

(RQ4) Develop interventions for aiding users in mitigating attacks.



Acknowledgement:

This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSN).



Project Description

The Challenge

- IoT deployments in healthcare and industry rely on heterogeneous wireless protocols (Zigbee, Z-Wave, Bluetooth, Wi-Fi), each introducing distinct attack surfaces that threaten patient safety and industrial continuity.

Our Approach

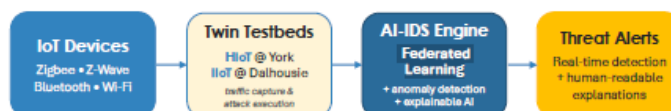
- Build a unified, AI-powered Intrusion Detection System (IDS) that combines behavioral analysis, anomaly detection, and federated learning to detect evolving threats across protocols, without compromising data privacy.

Twin Testbeds

- Industrial IoT (IIoT) testbed at Dalhousie University: smart factory and automation scenarios.
- Healthcare IoT (HIIoT) testbed at York University: remote monitors, wearables, infusion pumps.

Project Team

- Five investigators from Dalhousie University and York University.
- Funded by NCC, Call for Proposals 2025, Spearhead R&D project.



Current Progress

Where We Are:

- Comprehensive literature review of IoT protocols and AI-based IDS methods and gap analysis.
- Testbed design: device selection, network architecture and threat scenarios defined for both HIIoT (York) and IIoT (Dalhousie) sites.
- Data-collection framework prototyped; preliminary labelled datasets generated from baseline traffic captures.
- Foundational AI threat-detection model under development using anomaly detection and predictive modelling.

Project Collaborators

Investigators

Dalhousie University

Faculty of Computer Science

- Samer Lahoud
- Srinivas Sampalli
- Nur Zincir-Heywood

York University

School of Information Technology

- Arash Habibi Lashkari
- Xiaohui Yu

Threats We Detect

Man-in-the-Middle

Denial of Service

Spoofing

Trojans / Backdoor

Rogue Access Point

Packet Sniffing

Budget & Method

Project Budget

\$924K Total project cost

\$443K Requested from NCC

\$480K Matching contributions

Method

- Build twin protocol-aware testbeds (HIIoT & IIoT); capture benign and malicious traffic across Zigbee, Z-Wave, Bluetooth, Wi-Fi.
- Curate four open, annotated IoT-attack datasets for the research community.
- Train a federated, explainable AI-IDS with integrated dashboard; validate against MITM, DoS, spoofing, rogue APs, malware.

Future Exploration

What's Next

- Integrate Explainable AI into the detection framework: local & global threat interpretation.
- Develop modular, protocol-aware traffic analyzers as open-source tools.
- Validate prototype in real-world hospital and factory pilots with industry partners.
- Engage standards bodies (NIST, IEEE, ISO/IEC, ...) to inform IoT security guidelines.
- Train HQP: 10 graduate students (5 PhD, 5 MSc) across Dalhousie and York.
- Dissemination: 3 webinars, 1 policy brief, stakeholder roundtable, peer-reviewed publications.



Acknowledgements

This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (GCN). Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (GRC).

With thanks to Dalhousie University, York University, and the project's industry and academic partners.

Cyber Resilient Battery Management System with secure Bi-directional Power Flow for Connected Vehicles

Sheldon Williamson (PL), Professor and Canada Research Chair Alumni,
Ontario Tech University, Oshawa, ON. Sheldon.williamson@ontariotechu.ca



Project Description

Project Focus:

- Develop a cyber-resilient Battery Management System (CR-BMS) for electric vehicles (EVs).
- Design secure Vehicle-to-Grid (V2G) power control architectures.
- Protect EV batteries, charging infrastructure, and grid-connected energy transactions from cyber threats.
- Support Canada's clean transportation, smart grid, and critical infrastructure security goals.

Goals & Key Milestones:

- Design a secure BMS architecture for EV charging infrastructure.
- Develop AI-based intrusion detection for EV charging and battery management systems.
- Implement secure authentication and resilient bi-directional power control.
- Create an EV cyber-risk assessment and testing framework.

Project Collaborators

- **Co-Lead: Dr. Mohammadreza Arani,**
Toronto Metropolitan University (TMU)
Assistant Professor and Canada Research Chair
Smart Grid Cyber-Physical Security, Toronto
Metropolitan University, Toronto, ON.
- Postdoctoral Fellow: Dr. Varaprasad Oruganti,
Ontario Tech University, Oshawa, ON.
- Graduate Student: Mohit Sharma,
Ontario Tech University, Oshawa, ON.

Budget & Method

Total Budget granted from NCC: \$500,000 CAD

Method:

- ✓ Conduct a comprehensive review of EV cybersecurity, BMS vulnerabilities, and V2G threats.
- ✓ Develop simulation and experimental platforms for BMS and V2G testing.
- ✓ Design secure communication, authentication, and firmware management frameworks.
- ✓ Develop AI-based anomaly detection and cyberattack mitigation strategies.
- ✓ Validate solutions through cyberattack scenarios and resilience testing.

Current Progress

Project Status (April 2026 – Present):

Completed / Ongoing Activities

- ✓ Literature review on EV cybersecurity, BMS security, and V2G vulnerabilities.
- ✓ Establishment of project infrastructure for BMS and V2G research platform.

Key Contributions:

- ❖ Mapped cyber threats affecting battery systems and bi-directional charging.
- ❖ Initial architecture concepts for the cyber-resilient BMS.

Lessons Learned:

- ❖ Existing BMS solutions emphasize performance and safety but not cybersecurity.
- ❖ V2G systems introduce significant new attack surfaces through connected infrastructure.
- ❖ Current cybersecurity assessment methods are not tailored to EV-grid interactions.
- ❖ Integrated cyber-physical protection is essential for future EV ecosystems.

V2G Configuration



Future Exploration

Next Steps (TRL 3–5)

- Develop AI-driven intrusion detection models using simulated attack datasets.
- Design resilient V2G control algorithms with cyberattack mitigation capabilities.

Additional Research Needs

- Validation against emerging EV cybersecurity standards and regulations.
- Development of advanced cyber-physical attack test scenarios.

Project Growth & Impact

- ✓ Transition from simulation to hardware-in-the-loop and prototype validation.
- ✓ Contribute to Canadian EV cybersecurity standards and best practices.
- ✓ Train highly qualified personnel in transportation electrification and cybersecurity.

Acknowledgements



This project was made possible through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).



Reliable Machine Learning for Android Malware Detection

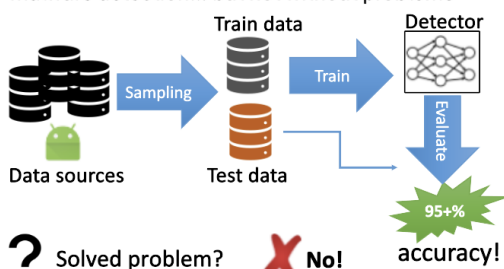
Michael Tegegn and Julia Rubin, The University of British Columbia, Vancouver

Contact: mtegegn@ece.ubc.ca, mjulia@ece.ubc.ca



Project Description

Machine learning is widely adopted for Android malware detection... but not without problems



Problems/biases:

- Sample duplication
- Temporal bias
- Label inaccuracy
- Label inaccuracy

Objectives:

- Investigation
 - Characterization of feature sets and datasets used
 - Empirical evaluation of existing approaches
- Solutions
 - Propose reliable feature sets, data selection methods, and learning approaches appropriate for software / malware
 - Devise an explainable malware detection approach

Project Collaborators

- Julia Rubin and Michael Tegegn
- ReSeSS Lab, The University of British Columbia, Vancouver campus

Budget & Method

Budget

- Total Project Funding: \$262,200 CAD over 3 years, used mostly to fund graduate student salaries
- NCC Contribution: the entire amount
- Anticipated Match: 0 (Spearhead project)

Method

- Carried out through analysis and development phases

Literature review + analysis Review features, datasets, evaluations	Representation learning Improve featurization and data processing
Empirical Evaluation Use curated datasets to evaluate tools	Explainable detection Investigate best algorithm for software
Dataset investigation Study how data properties impact success	Industry outreach Collaborate to test on industry challenges

Current Progress

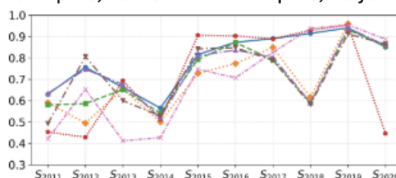
M1: Conducted a large-scale literature review of detectors [1]

Venues: = 157 papers
46 major

TLDR: Several approaches, with their own evaluation configs

M2: Carrying out a large-scale evaluation [1] [in progress]

- >150K samples, 18 walk-forward splits, 13 years span



TLDR: Tools results range from 98% to 40% even on different splits of the same "clean" datasets.

M3: Investigating dataset characteristics [in progress]

- Concept drift analysis via clustering

TLDR: Clusters exist, incidence in train/test dictates results

Future Exploration

Building a reliable Android malware detector

Data Preprocessing

- How to prune irrelevant information from apps?

Malware ~ 10K+ methods, 1M+ tokens
Malicious payload ~ few hundred tokens

Feature Engineering

- How to extract semantic features?

Non-semantic features → Spurious correlations

Algorithm Design

- How to frame the malware detection problem?

Malware vs Benign ≠ Cats vs Dogs

Explainability

- How to make tool results traceable to code?
- How to explain tool results to analysts?

List of APIs ≠ Code traces capturing behavior
APIs + Weights ≠ Actionable analysis reports



Where and how to incorporate LLMs into the steps above?

Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).

Talent and Workforce Development



Mobilizing Cybersecurity Regulation for Canada

Lyndsay Campbell, Professor, University of Calgary



Project Description

We are preparing lawyers and legal academics to meet the legal challenges intertwined with cybersecurity, by educating them on **privacy, international trade, financial crimes, human rights, intellectual property, financial technologies, national security, critical minerals, legal history, and artificial intelligence**.

We are:

- Giving students experiential learning opportunities with industry, government and academia
- Expanding course and mooted offerings
- Working toward additional transdisciplinary graduate-level credentials in cyber- and national security
- Educating and supporting the next generation of legal academics

Team:

- Emily Laidlaw, PhD – Internet Law, Cybersecurity, Privacy, Human Rights
- Michael Nesbitt, PhD – National Security
- Greg Hagen, PhD – Intellectual Property, IT
- Elizabeth Whitsitt, PhD – International Trade, International Economic Law
- Gideon Christian, PhD – AI, Legal Practice
- Sanaa Ahmed, PhD – Financial Crimes, Money Laundering
- Elizabeth Steyn, PhD – Critical & Strategic Minerals
- Lyndsay Campbell, PhD – Project Lead and Legal History

Contact:

Lyndsay Campbell: lcampbe@ucalgary.ca

Budget & Method

Budget:

Total project cost: \$1,291,272.34
NCC contribution: \$915,838.15
Matching: \$375,434.19

Method:

- Bringing in government and industry experts to teach new courses and enrich existing ones
- Supporting postdoctoral researchers and graduate students working in the area
- Sending students to conferences and moots
- Offering research opportunities to our students

Current Progress

Hosted “Cyberthreats to Canadian Democracy” academic-industry-government conference: subject experts plus graduate students and a postdoc presented (Aug/25).

Hosted “Critical Minerals Challenges for the Digital Transition” industry-academic workshop: subject area experts plus JD and graduate students presented (Nov/25).

JD and LLM students presented in other venues as well. New courses were offered. New graduate programming is under development.

Two postdocs, 4 PhD students and 12 LLM students conducted and presented research, contributing to the project goals. Five LLM students defended their theses, 2 PhD students advanced to candidacy, and a JD team competed in the Harold G. Fox IP moot.

Future Exploration

As we move into the final year of the grant, students at the PhD, LLM and JD levels will continue to engage in experiential learning opportunities and research projects related to their interests, acquiring valuable expertise in the legal environment that shapes cybersecurity and society’s responses to its challenges.

A postdoc continues to research cybersecurity, terrorism and illicit finance. Two PhD students should advance to candidacy in 2026-27 doing research on 1) AI’s use in arbitration and warfare and 2) the legal framework governing critical minerals required for quantum computing.

LLM students are conducting research on topics including privacy and healthcare data; cybersecurity and the Internet of Things; data poisoning and copyright; and the right to be forgotten.

Progress has begun on an edited collection showcasing the best papers from the last three years’ critical minerals workshops.

New graduate-level program will move through university and government approval processes.

Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).

We are grateful to the Faculty of Law for its support.



Cyber Lab

Noel Murphy, Field Effect
nmurphy@fieldeffect.com



Project Description

A national, web-based cyber range ecosystem delivering hands-on labs and supported by a community of content developers.

Project Focus

- Launch scalable, browser-based cyber range
- Curate/publish labs, assessments & exercises
- Integrate with LMS for automated enrollment/results

High-Level Goals & Milestones

- Deploy Cyber Range to partner organizations
- Develop a catalog of 130+ labs, 8 capstone scenarios
- Enable LMS integrations (Canvas, Blackboard, etc.)

Team Undertaking It

- Field Effect
- Post-secondary academic institutions
- Workforce retraining non-profits
- Academic-commercial partnerships

Context / Landscape

- Addresses national hands-on cybersecurity training gap
- Replaces ad-hoc lab environments with a seamless browser experience
- Meets industry demand for job-ready grads with practical skills

Project Collaborators

- Algonquin College
- University of Calgary
- Information and Communications Technology Council (ICTC)
- Dalhousie University
- University of Ottawa
- Carleton University / General Dynamics Mission Systems

Budget & Method

- Project approval in 2023, started in 2024
- \$900,000CAD in committed funds from NCC

4-year project with 7 milestones:

- **M1:** Engage with partners, establish curriculum needs
- **M2:** Onboard initial partners with range and content
- **M3-M5:** Create training based on M1 learnings
- **M6:** Create public repository of content that partners can easily load content from
- **M7:** Modify the Cyber Range to support infrastructure commonly used by academia

Current Progress

The Cyber Range platform supports authoring, administering and consuming courses and exercises, both self-paced, individual instructor-led and group-based exercises. The platform is being used for custom exercise / scenario development and capstone exercises. The catalog of included material continues to be expanded.

To date, 43 labs, 20 full courses and 4 team exercises have been completed.

The completed material covers topics such as:

- Windows Active Directory Hardening
- Linux Security Foundations
- Web Application Penetration Testing
- Ethical Hacking
- Post-Incident Recovery
- Red Team Activities
- Malicious PowerShell Analysis

Partner organizations are deploying hardware and prepping for fall semester rollout of material as needed for various programs

Future Exploration

Staying current in cybersecurity is always paramount. Continue working with partners to understand the future of their programs and ensuring the learning material being developed reflects the programs offered.

As a cybersecurity vendor, Field Effect has first-hand knowledge of real-world incidents and malicious actors and uses this to ensure new materials reflect what students need to know today.

The project is open to more partnerships.

Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).

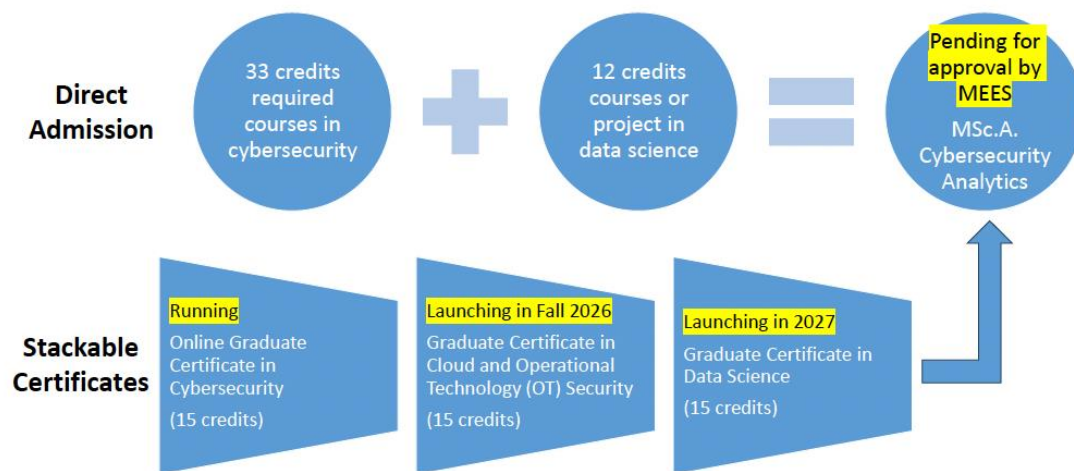


Hybrid Master's Program in Cybersecurity Analytics

Pls: Benjamin Fung and Steven Ding
School of Information Studies, McGill University



Cybersecurity Analytics = Cybersecurity + AI



Progress and Projection

- Enrolment in Graduate Certificate in Cybersecurity 2022: 17 | 2023: 31 | 2024: 62 | 2025: 60 students
- Enhanced 5 online cybersecurity courses and creating 6 new in-person cybersecurity courses with hands-on interactive lab activities
- Launching Graduate Certificate in Cloud & OT Security in Fall 2026.
- New Graduate Certificate in Data Science will launch in 2027.

Project Collaborators

- EC-Council: interactive lab activities
- Hex-Rays: Provide software reverse engineering tools

Budget (\$2.4M)

NCC = \$1M | McGill \$1.3M | EC = \$78K | Hex-Rays: \$26K

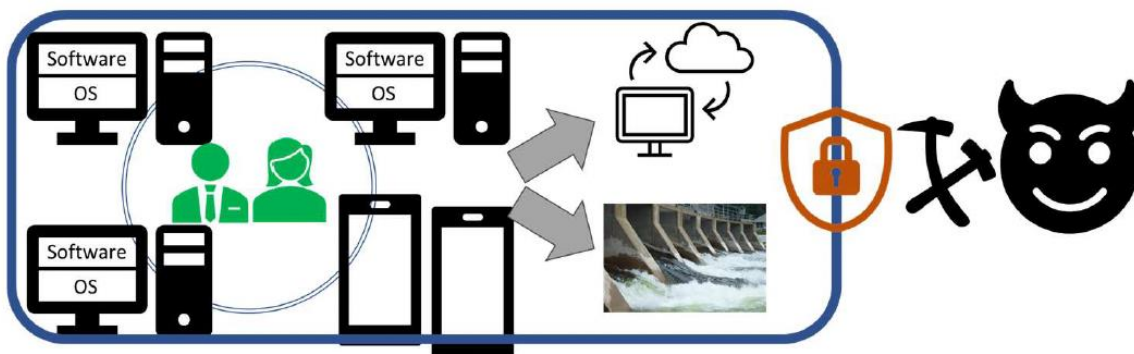
Approvals

- Approved by
- McGill School of Information Studies
 - McGill Faculty of Arts
 - McGill Committee of Graduate and Postdoctoral Studies
 - McGill Senate

Pending approval by:

- Ministère de l'Éducation et de l'Enseignement supérieur (MEES) / Ministry of Education and Higher Education of Quebec (Expected: 2027)

Gaps: Basic Cyber + Cloud & OT Security + AI



Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).

Cybersecurity Management Master

Luigi Benedicenti, University of New Brunswick,
 luigi.benedicenti@unb.ca

Program Director:
 Akash Das
 UNB
 akash.das@unb.ca

Project Description

The project aims at creating a Master of Cybersecurity Management program. Some of its most salient features are as follows:

- The program sits at the intersection of executive **cyber governance** upskilling and flexible online **professional education**, directly addressing a structural **Canadian shortage** of non-technical cybersecurity leaders while filling a **clear gap** in Canada's postsecondary market for fully online, governance-focused master's programs priced and structured for working professionals.
- Project milestones include an **academic component** (market analysis, curriculum development, test runs and refinements, approvals) and a **management component**.
- The project team comes from three faculties: **Computer Science, Law, and Management**, to ensure all aspects of cybersecurity management are included.
- The program delivery will be **flexible**, mostly if not fully **online**, to offer ease of attendance to working professionals (upskilling).

Project Collaborators

- Faculty of Computer Science: Luigi Benedicenti, Saqib Hakak
- Faculty of Law: Michael Marin, Argyri Panezi
- Faculty of Management: David Foord, Devashis Mitra
- Program Director/Project Manager: Akash Das

Budget & Method

Budget:

- Total Project Budget: \$2,585,110
- NCC Contribution: \$998,538
- Matching Contribution (UNB): \$1,586,572

Method:

- The project is managed by a **program director**, responsible for coordinating work among the three faculties.
- The project is divided into **stages**: market analysis, curriculum ideation, course development, testing and refinements, and program approval.

Current Progress

- After a rocky start due to the difficulty in hiring a program director, and an adjustment in the project schedule, **program development is now on track**.
- The project director and the PI identified **program champions**, who possess the specialized knowledge and expertise to create and deliver a **tailored curriculum** for the program.
- The **market analysis** was completed; its results suggest that the target audience might need to be expanded by including **leadership components** into the curriculum.
- Currently, the team is working on **curriculum development**, which has changed since the project started as AI has become prominent in cybersecurity and most other aspects of IT.

Future Exploration

- The next step is crucial to the success of the project: **curriculum development** and the **learning objectives** it contains are the cornerstone of the whole program.
- After curriculum development, **course development** will be next. This will happen in two phases: an **initial** course development effort involving instructional development, and a **refinement** phase after the course has been taught at least once.
- All courses will be **piloted** at least once to test their effectiveness and fit into the program. Any issues will be recorded and used to refine the courses and/or the curriculum.
- Finally, **academic approvals** will be sought at the faculty level, then Senate, Board of Governors, and Province.
- While seeking Provincial approval, **program marketing** will begin to attract students into the new program.

Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).

Accelerating Efforts to Secure Canada in an Era of Quantum

Quantum Algorithms Institute

Project Description

The advent of commercial quantum computing has foregrounded the serious cybersecurity threats expected in the coming years. A fault-tolerant quantum computer could break the mathematical challenges that underlie current digital encryption protocols in a matter of hours or even seconds. The Canadian Centre for Cyber Security has noted that threat actors can steal encrypted information now and hold on to it until a sufficiently powerful quantum computer is available to decrypt, read, or access the information, even well after the information was created. With significant investments being made into commercial quantum computing around the globe by governments, industry, and investors, and with breakthroughs reported every week, there is an urgency to help Canadian organizations prepare for these threats.

To address this urgent need, the Quantum Algorithms Institute (QAI) has created quantum cybersecurity and professional development teams. In partnership with industry, government, education, and non-profit organizations across Canada, QAI will deliver training for cybersecurity professionals and leaders from various sectors and help implement best practices. Over the next four years, the investment from the National Cybersecurity Consortium, QAI and its partners will result in hundreds of organizations across Canada embarking on their journey to become quantum safe.

Project Collaborators

- Field Effects
- ICTC
- siberX
- Canadian Information Processing Society
- Beauceron Security
- Quantum Algorithms Institute
- Durham College

Budget & Method

- NCC's contribution: \$1,000,000
- Cash contribution: \$475,000
- In-kind contributions: \$1,064,000

Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).



Project Description

Context / Landscape

- Cybersecurity workforce demand far exceeds supply, especially for roles beyond purely technical functions.
- Traditional training often ignores human, legal, and organizational dynamics of cyber incidents.
- Canadian and international regulations (e.g., Bill C-27, Bill C-26, Québec's Loi 25, GDPR) require cross-disciplinary understanding of compliance and response.
- AI is reshaping the cyber threat landscape, necessitating new approaches to defense and decision-making training.

Project Focus

- Develop immersive, human-centric cybersecurity training simulations for non-technical professionals.
- Address socio-technical and legal implications of cyberattacks using real-world, AI-driven scenarios.
- Leverage the uOttawa-IBM Cyber Range (Ottawa) and CATE (Calgary) to deliver high-impact training across Canada.

Multidisciplinary Team

Lead Institution: University of Ottawa

• Prof Guy-Vincent Jourdan (Engineering)

• Prof Céline Castets-Renard (Law)

• Prof Kathryn Prince (Arts)

• Latifa El Bargui (Engineering)

• Julien Cassagne (Engineering)

• Ayman Naciri (Audiovisual)

• Sarah Gabad (Law)

Co-Lead: Université de Montréal

• Prof Benoit Dupont (Criminology)

• Charlotte Burelle (Criminology)

High-Level Goals & Milestones

- Create a catalogue of 6 realistic, multidisciplinary training scenarios.
- Deliver these scenarios to over 1,000 professionals during the project period (2025–2028).
- Disseminate materials in both official languages and share content freely with Canadian academic institutions.

Future Exploration

Growth Potential:

- Expand delivery across Canada through partner institutions equipped with compatible cyber range platforms.
- Explore international deployment of bilingual scenarios, especially in Francophone countries.
- Future funding and partnerships will support new scenario development (e.g., post-quantum threats, misinformation campaigns).
- Research component to be developed, studying the impact of the developed scenarios on various populations.

Budget & Method

Total Budget: \$3.47M over 4 years

NCC Contribution: \$961,400

Matching Contributions: \$2.5M (cash and in-kind from universities and industry partners)

Delivery Method:

- Scenarios developed using a rigorous, iterative process.
- Training delivered at two national cyber ranges (uOttawa-IBM Cyber Range and CATE in Calgary).

Execution Plan:

- Six immersive cyberattack scenarios created through multidisciplinary collaboration (law, tech, theatre, criminology, education).
- Each scenario progresses through phases: discovery, build, controlled delivery, refinement, training, and steady-state rollout.



Current Progress

Scenario #1:



Scenario #2:



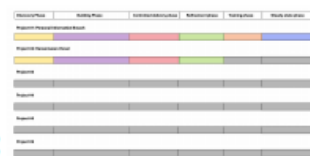
Project Collaborators



Acknowledgements

This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (GCN). Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RCC).

Add any other acknowledgements as appropriate.





Marine Cybersecurity



Jonathan Anderson, Memorial University of Newfoundland
jonathan.anderson@mun.ca



SCMS: Securing Critical Marine Systems NCC 2024-1326

Canada's is dependent on the maritime sector and exposed to vulnerabilities in marine control systems. This project will:

- develop **protocols** and **platforms** for trustworthy, resilient marine systems
- prototype electronic navigation and control systems with hardware and/or software compartmentalization (e.g., Capsicum, CHERI, CHERIoT)
- visualize cybersecurity state to seafarers
- demonstrate practical integration of secure systems on the water

Budget & Method

NCC	\$759,100
Memorial University	\$586,400
Dalhousie University	\$172,800
GovNL	\$138,806

- HQP support
- Marine equipment
- Research dissemination costs

SCMS Collaborators



Dalhousie University
Faculty of Computer Science



Current Progress

Control protocol (paper under submission)

Developing data-gathering "black box"

CSA TS-028: MASS Cyber



Stakeholder workshop inc. CCG, RCN

Future Exploration

Potential application for sensitive use cases with a new partner (platform vendor)

Potential expansion to protection of naval control protocol via DDS and Modular Open Systems Architecture (MOSA)

Potential collaboration with another Canadian university



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).

These projects were also made possible by matching contributions from Memorial University and Dalhousie University.

Acknowledgements

MCT: Marine Cybersecurity Training NCC 2024-1354



Over 80% of international trade is carried by maritime transport, with over 100,000 vessels of 100 gross tons or more, crewed by over 1.9M seafarers around the world. Seafarers undergo extensive training, but not on cybersecurity. This project will develop three training modules:

1. Cybersecurity essentials for the marine industry (both seafarers and shore side)
2. Intensive, simulator-based emergency procedure training for seafarers
3. Corporate emergency procedure training and validation (table-top)

Budget & Method

NCC funding:	\$576,528
Memorial matching:	\$578,699

- HQP support
- Simulation and technology costs
- Research dissemination costs

Current Progress

Team recruitment and preparation for simulation work (collab. with NRC project)



Site visit by vessel operator interested in piloting our training courses

Future Exploration

Relationship to emerging global MASS code (Marine Autonomous Surface Ships)

Impact on global seafarer training standards

Potential expansion to naval use cases

MCT Collaborators



IncidentSync

Bridging IT and Law Enforcement Training

Project Lead: Herbert Fensury
herbert.fensury@enfocom.com

For additional information
 go to www.enfocom.com
 Email: info@enfocom.com

Project Description

Timeline: Mar 31, 2025 – Mar 31, 2028

Environment

- Organizations and law enforcement agencies often approach cyber incidents investigations differently, leading to confusion and delays during post-incident response.
- IncidentSync addresses this gap with a unified framework of clear policies and procedures to guide collaborative response efforts.

Project Focus

- Strengthen collaboration between organizations and law enforcement.
- Develop a shared post-incident framework to align policies and procedures.
- Train stakeholders with skills and knowledge to respond effectively and cohesively to cyber incidents.

Goals & Milestones

- Unify response protocols:** Develop a comprehensive framework to guide coordinated post-incident actions.
- Enhance communication:** Establish shared terminology and expectations to support seamless coordination.
- Build capacity through training:** Deliver targeted training to ensure consistent application of the framework across sectors.

Team

- Led by ENFOCOM Cyber with proven law enforcement cybersecurity training experience.
- In partnership with:
 - Local & national law enforcement agencies.
 - Academic & professional training institutions.
 - Cybercrime & cybersecurity training experts.

Project Collaborators

Law Enforcement Agencies

- Calgary Police Service (CPS)
- Edmonton Police Service (EPS)
- Royal Canadian Mounted Police (RCMP)

Academic & Professional Training Institutions

- Toronto Metropolitan University – Rogers Cybersecure Catalyst
- University of Ottawa
- Université du Québec en Outaouais
- University of Calgary - Continuing Education
- InceptionU Educational Foundation Ltd.
- Savvy Knowledge Corporation

Cybercrime & Cybersecurity Training Experts

- Field Effect Software Inc.
- IBM Canada
- Intlabs

Current Progress

- Needs Assessment:** Identified post-incident procedure gaps through state-of-the-art framework analysis, surveys, interviews, and incident analysis.
- Workshops:** Facilitating hands-on workshops with stakeholders to co-create the first draft of a practical, context-aware framework.
- Partnerships:** To support coordinated capacity-building efforts, national-level collaborations have been established with some federal and provincial police agencies and private organizations.

Key Learnings & Adjustments

- Identified gaps in the state-of-the-art post-incident frameworks.**
- Scope Refinement:** Adjusting the development scope of the unified post-incident response framework based on assessment findings, expanding participating organizations to ensure more holistic and diverse review, with stronger engagement from legal and government stakeholders.
- Training Program:** Changes to the training program curriculum for a comprehensive program aligned with the unified framework.

Budget & Method

Total Budget: \$7,411,884 CAD

NCC Funding Request: \$1,000,000 CAD, allocated as:

- Unified Framework Development and Research (25%)** - \$250,000
- Training Program Development (30%)** - \$300,000
- Program Delivery & Implementation (20%)** - \$200,000
- Promotion and Outreach (10%)** - \$100,000
- Operational Costs (15%)** - \$150,000

Methodology

- Develop clear, consistent **policies and procedures** for post-incident response.
- Deliver **training** to equip stakeholders with the skills to apply the framework collaboratively.
- Strengthen **public-private coordination** through shared language and aligned expectations.

Future Exploration

Next Steps

- Complete the **development of a unified post-incident framework** integrating industry best practices and law enforcement insights.
- Create a training program** based on this framework for effective incident response.
- Deliver the training** to companies, organizations, and law enforcement agencies.
- Offer nationwide certification** through partner organizations.
- Promote the adoption of standardized incident handling procedures** to foster collaboration and efficiency.

Expansion Opportunities

- Scale Up:** Roll out the framework and training programs nationally through existing and new partnerships.
- Collaborate:** Grow partnerships with associations, academia, and industry to promote the framework and training.
- Integrate:** Embed the developed training into current programs.
- Go Digital:** Launch an on-demand learning platform.
- Empower:** Deliver train-the-trainer programs for local reach.
- Adapt:** Continuously evaluate and refine the framework and the training.



Acknowledgements

This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSNI).
 Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RCC).



Phishing, Smishing, Vishing

David Knox, University of Ottawa, dknox@uottawa.ca



Project Description

- **Social Engineering attacks that target people** are on the rise in Canada and globally
- **More effective educational tools** are needed, requiring a **multi-disciplinary** approach, for the design of appropriate remedies, using **modern education technologies** and methods
- Detailed understanding is required of:
 - People and how they behave as **victims**
 - **Social Engineering Attacks** (e.g. sextortion) and how they are adapted over time
 - Effective education techniques for **'difficult' topics** with disinterested learners (youth demographic and "support network")
 - Appropriate **modern media synthesis** for (effective) **online** educational technology
- **GOAL:** Design effective and innovative online educational treatments to make Canadians more resilient to online Cyberattacks launched against them, rather than their computing equipment.

Project Collaborators

- **Irene Vitoroulis:** UOttawa psychology professor ("victimization") co-prime
- **Selbi Kurbanova:** UOttawa forensic psychology doctoral student
- **Kainia Cloutier:** Faculty of engineering Secondary School (FESS) teacher
- **Julie Olivier:** Faculty of engineering Secondary School (FESS) principal
- **Vignesh Karuppasamy:** engineering masters student (just graduated!)
- **Sean MacKenzie:** UOttawa engineering masters student (and RCMP employee)
- **Dave Bosasi:** UOttawa engineering masters student (and Nokia employee)
- **Sumit Paul:** UOttawa engineering doctoral ("Privacy") student (just graduated!) too!
- **Kristina Stanley:** Fiction-writing expert consultant and CEO of "Fictionary"
- **Alexandria Connolly, Mauranne Ste.-Marie:** RCMP Sensitive and Specialized Investigative Services unit
- **David Knox:** UOttawa engineering professor ("cybersecurity education") and prime

Budget & Method

- Total project budget: **\$373,500**
- "In-kind" contributions from the RCMP: **\$15,000**
- The project has three phases, organized around three different attack vector mediums:
 - **Phishing:** A social learning game ("Phooled!") has been developed and compared with more traditional solitary online teaching methods. Multi-year study of motivation for learning has been conducted with first-year engineers (i.e. 17-year olds)
 - **Smishing:** Existing carrier-based detection tools will be evaluated in both French and English. Novel and adaptive user-based tools will then be developed and tested.
 - **Vishing:** Story-telling game-based learning tool for sextortion types of attacks developed, called "StarFall", with AI-generated media outputs and a social learning component, combined with a reflective/synthetic activity that allows the education treatment to evolve over time. The RCMP has been tracking sextortion attacks against minors as a distinct, growing, attack type against minors

Current Progress

- **Phishing:** "Phooled!" game has been live, as a public web. App. for most of 2025/6 (see the URL above to try it yourself!)
 - Tested with IT professionals and High-School-aged children
 - ASEE '25 motivation paper presented
- Practical "Privacy-preserving" Client/Server Mechanism (for 'sensitive' data storage) designed and published
- **Smishing:** Initial experiments show Canadian carrier-based malicious SMS detection worse than 40% !
- **Vishing:** Initial experiments with high-school-aged children at the end of 2024 showed that (free) generative AI audio synthesis technology is currently more effective for education than AI-based (free) video synthesis technology. Scheduled for second phase of testing in June 2026

Future Exploration

- Social Engineering attackers adapt their attacks, in real time, to both maintain their effectiveness, but also to reduce the required attacker effort
 - Defensive education must keep up with these changes and evolve *by design!*
- Audio synthesis technology to "bring a story to life" seems ready for use in online education, but our tools will need to be revised and retested, based on their qualitative and quantitative effectiveness, after being redeveloped and re-tested (based on alpha testing)
- AI-based video synthesis tools are currently becoming much more effective and realistic
 - Deep-fake technology is now being used in attacks that target girls, specifically!
 - Boys are over-represented in sextortion attacks, currently
 - Our prototype testing, with high-school-aged students, showed that current video-synthesizing technology was "unconvincing", as an educational aid, but we want to revisit this technology, in the near future
 - We are evolving our research and tools to also target the "support network" of potential victims, since "victim isolation" and "grooming" have become common attacker strategies and education is not going to "reach" all potential victims, given the assumed 'reluctant learner' model
- A dyadic study of victims and their support network partners is now underway (at the recruitment and interviewing phase)

Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).

Parcours Cyber Action : Cybersecurity Training for SMEs

Daniel Chamberland-Tremblay, Danièle Normandin, Andrew Turk | Cybersecurity
Expertise Hub, Université de Sherbrooke | pole.cybersecurite@USherbrooke.ca



Project Description

- SMEs remain vulnerable to cyber incidents and often lack training tailored to their reality.
- The Parcours Cyber Action develops short, concrete, and accessible video capsules designed to strengthen cybersecurity habits.
- The content is custom tailored towards different roles, business sectors, and levels of maturity.
- The project is led by the Cybersecurity Expertise Hub of the Université de Sherbrooke alongside industrial and distribution partners.



Project Collaborators

- **Intact Insurance** : Financial and distribution partner
- **Cybereco** : SME contacts, needs assessment, field testing (focus groups)
- **Ludifilm** : Video production studio, Sherbrooke (QC)
- **Illuxi** : Distribution partner

Budget & Method

- Funding shared between :
 - CNC/NCC - \$580,679 cash
 - Intact Insurance - \$200,000 cash
 - Cybereco - \$75,000 in-kind
 - Multidisciplinary approach involving five faculties of the Université de Sherbrooke - \$305,679 in-kind
- TOTAL : \$1,161,358 / 4 years**
- Capsules scripted and produced in collaboration with a professional studio.
- Design of pedagogical content expertly crafted through extensive market research and the collected feedback from participating SMEs.

Current Progress

- Pedagogical architecture completed:
 - 5 personas
 - 18 modules
 - 73 learning units
- First video ("Phishing") in production.
- Content validation with experts and SME focus groups.
- Production partnership confirmed with Ludifilm.



Future Exploration

- Deploying the free common core training videos.
- Develop personalized learning paths by industry and function.
- Integrate an LMS platform with a scoring system and learning tracking with dashboards.
- Develop a semi-automated production pipeline that takes state-of-the-art Cybersecurity research and news, then converts it to certified training materials.
- Draft and implement the commercialization plan.
- Expand distribution across Canada.

Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).

The team also thanks all internal experts at the Université de Sherbrooke, as well as the partner companies for their collaboration in validating the content and defining the needs of SMEs.



Université de
Sherbrooke



Bridging the Law Enforcement Cybersecurity Training Gap

Project Lead: Herbert Fensury | ENFOCOM Cyber

✉ herbert.fensury@enfocom.com

For additional information go to
www.enfocom.com
Email: info@enfocom.com

Project Description

Timeline: Mar 31, 2025 – Mar 31, 2028

Environment:

- Cybercrime is increasing in volume and complexity.
- Police need trained cyber specialists.
- Travel costs or distance limit training access.
- CyberGuardian offers a national solution for equal access, stronger skills, and improved coordination across Canada.

Project Focus:

- Expand nationwide training program for law enforcement.
- Close cybersecurity skill gaps.
- Improve access to training, especially for remote and under-resourced agencies.

Goals & Milestones:

1. **Identify Needs:** Survey officers, review past cases, & spot gaps.
2. **Build Training:** Develop practical, role-specific programs.
3. **Expand Reach:**
 - a. Launch outreach campaigns & webinars.
 - b. Share easy-to-use learning materials.
 - c. Host & join events across provinces.
 - d. Partner with national police groups.
4. **Support Collaboration:** Connect agencies to share developed materials and expertise nationwide.

Team:

- Led by ENFOCOM Cyber with proven law enforcement cybersecurity training experience.

Project Collaborators

Law Enforcement Agencies:

- Calgary Police Service (CPS)
- Edmonton Police Service (EPS)
- Royal Canadian Mounted Police (RCMP)

Academic & Professional Training Institutions:

- Toronto Metropolitan University – Rogers Cybersecure Catalyst
- University of Ottawa
- Université du Québec en Outaouais
- University of Calgary - Continuing Education
- InceptionU Educational Foundation Ltd.
- Savvy Knowledge Corporation

Cybercrime & Cybersecurity Training Experts:

- Field Effect Software Inc.
- IBM Canada
- Intlabs

Budget & Method

Total Budget: \$7,264,619 CAD

NCC Funding of \$1,000,000 CAD, allocated as:

- **Needs Assessment & Research (20%)** - \$200,000
- **Training Program Development (30%)** - \$300,000
- **Partnership Building (30%)** - \$300,000
- **Outreach & Engagement (10%)** - \$100,000
- **Operational Costs (10%)** - \$100,000

Methodology:

1. **Identify law enforcement cybersecurity skill gaps** through surveys and roundtable exercises.
2. **Develop tailored cybersecurity training.**
3. **Build national partnerships.**
4. **Launch** outreach campaigns.
5. **Manage** tools, licenses, & operational costs.

Current Progress

Needs Assessment:

- Worked with several law enforcement agencies to identify cybersecurity training needs and gaps.
- A cybersecurity skills needs survey to identify existing gaps.

Partnerships:

- To support coordinated capacity-building efforts, national-level collaborations have been established with some federal and provincial police agencies and several professional training centers.

Key Learnings & Adjustments:

- **Clearer Skill Gaps:** Roundtables and survey analysis have revealed more precise insights into officers' training needs.
- **Refined Curriculum:** Proposed training programs and curriculum have been adapted to better align with real-world operational challenges.
- **Stronger Collaboration:** Roundtables and surveys have led to improved exposure to existing actors, national coordination, and more effective knowledge-sharing among stakeholders.

Curriculum Development:

- Monthly focus group meetings to build initial draft of the curriculum.

Future Exploration

Next Steps:

- **Refine Training Materials:** Continuously improve and expand training content based on participant feedback and evolving needs.
- **Strengthen Partnerships:** Strengthen ties with law enforcement agencies and training centres across Canada to enhance impact and reach.
- **Increase Outreach:** Increase the development and distribution of webinars, awareness campaigns, and educational resources.
- **Operations:** Ensure effective logistics, tools, and licensing management to support seamless program delivery.

Gaps & Learnings:

- **Training Needs:** Law enforcement officers require tailored, practical training that directly supports their operational responsibilities.
- **Access:** Access to high-quality training is often limited by cost, time constraints, and geographic inaccessibility, hindering skill development.

Expansion Opportunities:

- **Scale Up:** National rollout via current and future partnerships.
- **Collaborate:** Expand partnerships with associations, academia, and industry.
- **Integrate:** Embed newly developed training modules into existing training programs.
- **Go Digital:** Launch an on-demand online learning platform.
- **Empower:** Train-the-trainer programs for local training delivery.
- **Connect:** Build a Canada-wide community.
- **Adapt:** Continuously evaluate and update training.

Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).

Project Description

Despite the widespread recognition that employees are the weak link in organizational cybersecurity processes, the prevalence of errors, accidents, and oversights remains high. We posit that at the heart of this ongoing problem is a wide variation in the individual level of employee attention being directed towards cybersecurity activities.

This project will address the **managerial challenge of directing employee attention towards the fulfillment of day-to-day cybersecurity responsibilities**. Rooted in a human-centric view of cybersecurity, we seek to understand how fluctuations in employee attention to cybersecurity responsibilities relate to (in)secure behaviour.

Attention entails a focus of **time and effort** on both **cybersecurity issues** (e.g., recognizing a threat) and **answers** (e.g., following the procedures required to avoid the threat).

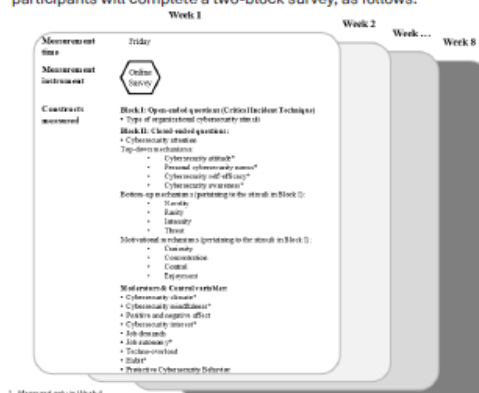
The first study in this research project consists of a **longitudinal study** that draws on theories of attention from the psychology, management, neuroscience, and economics literature, to investigate three categories of cybersecurity attention determinants:

- **top-down mechanisms** (i.e., cognitive responses);
- **bottom-up mechanisms** (i.e., sensory responses); and
- **motivational mechanisms** (i.e., pleasure responses).

Results from our study will offer insights regarding the relative importance of top-down, bottom-up, and motivational mechanisms in stimulating cybersecurity attention, alongside an improved understanding of the variability of week-to-week fluctuations in cybersecurity attention that represent organizational vulnerabilities.

Method

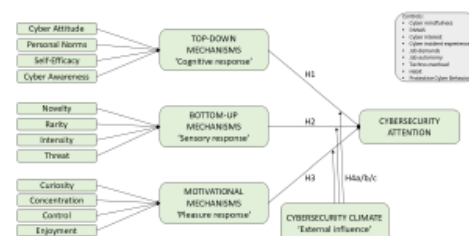
Longitudinal data will be collected using weekly surveys of approximately 300 (Canadian) participants using the Prolific research platform (www.prolific.com), over an eight-week period. Each Friday, participants will complete a two-block survey, as follows:



Acknowledgements

This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIS).
Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RCI).

Research Model



Project Collaborators

Our project team consists of the following researchers:

- Dr. W. Alec Cram, University of Waterloo (PI)
- Dr. John D'Arcy, University of Delaware (Collaborator)
- Dr. Alexander Benlian, TU Darmstadt (Collaborator)
- Ana Cezara Rusu, University of Waterloo (Research Assistant)

Current Progress and Budget

- Data collection commenced in early May and will continue until early July; data analysis is expected to be completed by the end of August.
- A conference paper is planned for presentation at the Americas Conference on Information Systems (AMCIS). A journal manuscript and teaching case study are expected to follow.

Expenses for the study include fees for data collection, research assistant salary, and travel for conference presentation. In total, expenses for this study are estimated to reach \$50,000 and are covered entirely by the NCC.

Future Exploration

This is the first of three studies investigating cybersecurity attention in organizations. Future studies are as follows:

- **Study #2** (2027-2028) will focus on Canadian cybersecurity professionals (e.g., analysts, managers, incident responders) to investigate how the volume and complexity of cybersecurity responsibilities impact employee attention during crises (e.g., cyberattacks).
- **Study #3** (2028-2029) will use case studies to investigate the challenges facing upper management and company directors at Canadian organizations. Specifically, we will focus on understanding how organizational leaders balance their attention to cybersecurity responsibilities alongside their corporate governance duties.



Critical Infrastructure Cybersecurity Experiential Training Program

Moein Manbachi, Ph.D., P.Eng., SMIEEE, Director
 Minoo Shariat-Zadeh, P.Eng., SMIEEE, Project Lead
 BCIT Smart Microgrid Applied Research Team (SMART)
minoo_shariat@bcit.ca



Project Description

This project develops a scalable, hands-on cybersecurity training platform to strengthen workforce readiness and resilience across Canada's critical infrastructure Operational Technology (OT) systems.

- **Focus:** Hands-on OT cybersecurity training via BCIT's Virtualized Experiential Learning Platform (VELP)
- **Goals:** Build workforce capacity; establish micro-credentials; deliver free accessible training games and modules
- **Team:** BCIT SMART in collaboration with utility & industry partners
- **Context:** Funded under NCC/CSIN 2025 – Critical Infrastructure Protection

VELP Training Hub



Three-Phase Delivery Plan:

Phase	Activities
P-1 (Assess, Q1-Q2 2026)	Needs assessment & training gap analysis; Curriculum and micro-credential framework design
P-2 (Build, Q2-Q3 2026)	Upgrade BCIT's VELP training platform; develop interactive learning modules; cybersecurity games; & launch an online learning portal
P-3 (Deliver, Q4 2026-Q1 2027)	Pilot training sessions & evaluation; culturally relevant training resources for Indigenous communities; knowledge dissemination

Budget & Method

Budget

NCC Grant (CSIN): \$310K
 Matching Contributions (BCIT and Partners): \$340K
Total Project Cost: \$650K

Training Method

- Hands-on learning in a safe virtual environment
- Co-developed with utility and industry partners
- Accessible and inclusive for Indigenous communities

Current Progress

- **Needs Assessment:** Engaged industrial stakeholders to identify training needs and workforce readiness gaps
- **Gap Analysis:** Reviewed existing training resources against industry standards; identified curriculum gaps & experiential learning opportunities
- **Curriculum Design:** Hands-on learning modules & micro-credential framework aligned with cybersecurity best practices
- **VELP Development:** Building interactive modules & OT cybersecurity games for engaging skills practice

Project Collaborators

Lead Institution

- British Columbia Institute of Technology (BCIT)

Industry Partners

- BC Hydro
- EdgeTune Power Inc.
- FortisBC

Future Exploration

- **Broader Rollout:** Expand platform and curriculum to additional critical infrastructure sectors beyond energy systems
- **Indigenous Training:** Adapt training materials for Indigenous communities and support community-based delivery models across Canada
- **Knowledge Transfer:** Share project outcomes through publications, conferences, workshops, and public webinars

Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).

Additional support provided by BCIT DTI-Hub and collaborating partners, including BC Hydro, Siemens Canada, and others.



DRIVING CYBERSECURITY EXCELLENCE

BUILDING PATHWAYS TO REDUCE LABOUR AND SKILLS GAPS

Derek Leung | Director, Innovation & Program Development | derek@digitalnovascotia.com

PROJECT DESCRIPTION

Goals

Develop new cybersecurity courses not available in market, upskill 150+ professionals, and develop stronger cybersecurity leadership across Canada.

Milestones include: Industry-driven curriculum design, public course launch, cohort delivery, participant supports, and national collaboration.

Project Focus

Close mid-career and senior **cybersecurity skills gaps identified by 3 out of 4 employers** through applied governance, risk, AI, and systems security training. national collaboration.

CURRENT PROGRESS

Cybersecurity Governance & Risk Management | Course Now Live

Developed to help experienced cyber and IT professionals translate technical risk into executive-ready strategy through applied training in governance, risk assessment, maturity modeling, cybersecurity roadmapping, and leadership communication.

AI & Security Systems | Course Now Live

Developed to help professionals secure AI-enabled environments by applying ISO/IEC 27001 and ISO/IEC 42001 to assess controls, identify AI and system risks, and build a practical security roadmap.

BUDGET & METHOD

- Total Project Value: \$997,925.42 (\$498,943.39, NCC + \$498,982.03 in matching partner contributions)
- Method: Industry-led curriculum design, academic expertise embedded, and leveraging partnerships and resources for experiential training

COLLABORATORS



Ken Muir

CISO/CSC/CISA/CRISC

- Top 100 Global Thought Leader
- Top 50 Who's Who in Cybersecurity
- Co-author, CIS Cybersecurity Framework V8

Academic and Regional Partners



WAT SPEED



Catalyst Community

FUTURE EXPLORATION

- Deliver and refine program using participant feedback, instructor insight, employer input, and labour market needs.
- Grow employer partnerships for mentors, panels, applied scenarios, work-integrated learning, and hiring pathways.
- Explore new stackable offerings in cyber leadership, AI governance, operational technology security, and risk communication.

First Response for Cyber Threats (FRCT) - A Collaborative Cybersecurity Training Initiative

University of Windsor

Project Description

The First Response for Cyber Threats (FRCT) is a national cybersecurity training initiative designed to help small and medium-sized businesses (SMEs) build defenses against digital threats. FRCT will empower businesses to train "cyber first responders" who can identify and act when cyberattacks strike, minimizing harm and disruption. FRCT offers three levels of training: basic awareness for all staff, technical defense for IT teams, and advanced threat response for security leads. A Train-the-Trainer pathway and mandatory recertification ensure lasting skills development and readiness within participating organizations.

The goal is to engage participants from sectors like construction, agriculture, energy, and manufacturing. To enhance hands-on learning, the project will develop a patented simulation software platform that tests responders in real-world cybersecurity scenarios.

By filling a national gap in SME-focused cyber training, FRCT will create a replicable and sustainable model to strengthen Canada's cybersecurity resilience and safeguard the digital economy.

Project Collaborators

- Sterling Information Technology
- WE-Tech Alliance

Budget & Method

- NCC's contribution: \$350,000
- Matching contribution: \$457,500

Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).

Preparing Canada's Workforce for the Future of Cybersecurity through Training and Academic Pathways

Project Leads: Professor Sherif Elbarrad, PhD, FCPA, FCMA, Dean, Mihalcheon School of Management, CUE, sherif.elbarrad@concordia.ab.ca; Eslam AbdAllah, PhD, Associate Professor and Chair, Information Systems Security and Assurance Management Department, Faculty of Management, CUE, eslam.abdallah@concordia.ab.ca.

Project Description

- Canada faces a widening cybersecurity skills gap, increasing risk for public, private, and community organizations. This project responds with flexible, online training for working professionals across Canada.
- CUE will develop 27 asynchronous cybersecurity modules, including 2 foundational modules that help learners without IT or cybersecurity backgrounds enter the learning pathway with confidence.
- The modules align with the seven core areas of CUE's MISSM program: Network Security; Application and Cloud Security; Cryptology and Secure Communications; System and Virtualization Security; Incident Response and Digital Forensics; Disaster Recovery and Business Continuity; and Governance, Risk, and Compliance. They are also informed by NIST CSF 2.0 and the Canadian Cybersecurity Skills Framework.
- The project supports upskilling, reskilling, career advancement, organizational resilience, and pathways into graduate cybersecurity education.
- The project builds on CUE's ISSAM expertise, public InfoSec seminars, industry relationships, and two decades of graduate cybersecurity education through the MISSM program.

Project Collaborators

CUE Project Team

- Shawn Thompson, MISSM, CISSP, Instructor / Program Liaison
- Cherry Mangla, PhD, Assistant Professor
- Dale Lindskog, PhD, Associate Professor
- Shaun Aghili, DBA, CMA(US), CISSP, CISA, CIA, CRMA, CFE, Professor
- Bobby Swar, PhD, CISA, Associate Professor
- Martin Higgins, PhD, Assistant Professor

Collaborating Organizations and Stakeholders

- ISC2 Alberta
- ISACA Edmonton
- OWASP Edmonton
- CyberAlberta Community of Interest
- Canadian Centre for Cyber Security

Budget & Method

- The project has a total budget of **\$661,000**, including **\$330,500 in NCC funding** and **\$330,500 in matching contributions from CUE**.
- Project implementation began in **Spring 2026**, with the development timeline focused on staged module design, review, and release.
- Development follows a staged model, moving from foundational and core cybersecurity content into technical, emerging, and advanced cybersecurity topics.
- Modules are designed for asynchronous online delivery through Moodle, supported by curated resources, practical activities, and alignment with industry-informed cybersecurity frameworks.

Current Progress

- Initial draft syllabi have been developed for **MCSC-1 to MCSC-6**, establishing early module structure, learning outcomes, and alignment with the overall pathway.
- Early resource review has begun for **MCSC-1 and MCSC-2**, with attention to current, accessible, Canadian-relevant materials for learners without technical backgrounds.
- The pathway has been refined into a **business-first progression**, moving from foundational learning to core, technical, emerging, and advanced cybersecurity topics.
- In June 2026, subject matter experts and instructors begin working with the development team to move approved module plans into Moodle-ready learning content.
- Early work has reinforced the need for clear entry points, practical activities, and accessible tools that support asynchronous learning for working professionals.

Future Exploration

- Move **MCSC-1 to MCSC-6** from draft syllabi and module plans into Moodle-ready content, activities, assessments, and learner supports.
- Expand development into the full **27-module pathway**, moving from foundational and business-focused cybersecurity learning into technical, emerging, and advanced topics.
- Strengthen cross-sector collaboration with industry, government, professional bodies, and community partners to ensure the modules reflect real workforce needs.
- Explore future undergraduate and graduate pathways that make cybersecurity learning more accessible across disciplines, including business, management, public service, health, education, and critical infrastructure.
- Support the NCC theme of **"Bridging Sectors, Securing Canada"** by helping make cybersecurity an integral part of professional education across sectors, not only a specialized technical field.

Acknowledgements



This project was made possible in part through the support of the National Cybersecurity Consortium and the Government of Canada (CSIN) // Ce projet a été rendu possible en partie grâce au soutien du Consortium national pour la cybersécurité et du gouvernement du Canada (RIC).

Add any other acknowledgements as appropriate.